XS3900-48F

48-port 10GbE Top-of-Rack Switch with 4-port 40GbE Uplink

Version 4.00
Edition 2, 4/2013

User's Guide

Default Login Details	
IP Address	http://192.168.0.1 (Out-of-band MGMT port) http://192.168.1.1 (In-band ports)
User Name	admin
Password	1234

Copyright © 2013 ZyXEL Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

'Switch' (title-case) refers to this product. Lower case 'switch' refers to switches in general.

Related Documentation

- Module Hardware Installation Guide

  This guide shows how to install and remove the power and fan modules in the Switch.
- Rack Mounting Hardware Installation Guide

  This guide shows how to use the rack mounting kit to install the Switch in a rack.
- CLI Reference Guide

  This guide explains how to use the Command-Line Interface (CLI) to configure the Switch.

Note: It is recommended you use the Web Configurator to configure the Switch.

- Web Configurator Online Help

  Click the help icon in any screen for help in configuring that screen and supplementary information.

Contents Overview

User's Guide 15

Getting to Know Your Switch 17
Tutorials 25
Switch Hardware Overview 49
The Web Configurator 53

Technical Reference 63

System Status and Port Statistics 65
Basic Setting 70
VLAN 81
Static MAC Forward Setup 99
Static Multicast Forward Setup 101
Filtering 105
Spanning Tree Protocol 107
Bandwidth Control 125
Broadcast Storm Control 128
Mirroring 130
Link Aggregation 132
Port Authentication 140
Port Security 148
Classifier 151
Policy Rule 157
Queuing Method 162
VLAN Stacking 165
Multicast 172
AAA 187
IP Source Guard 200
Loop Guard 220
VLAN Mapping 224
Layer 2 Protocol Tunneling 228
sFlow 232
PPPoE 236
Error Disable 244
Private VLAN 249
Static Route 253
Differentiated Services 256
DHCP 263
Maintenance 269

Access Control 276
Diagnostic 296
Syslog 297
Cluster Management 300
MAC Table 306
ARP Table 309
Configure Clone 311
Troubleshooting 313

Table of Contents

Contents Overview **3**

Table of Contents **5**

Part I: User's Guide **15**

Chapter 1
Getting to Know Your Switch **17**

1.1 Introduction 17
1.2 Data Center Bridging (DCB) 17
1.2.1 PFC, ETS, and DCBX Standards 18
1.2.2 DCB Configuration 19
1.3 Bridging Example 21
1.4 High Performance Switching Example 22
1.5 IEEE 802.1Q VLAN Application Example 22
1.6 IPv6 Support 23
1.7 Ways to Manage the Switch 23
1.8 Good Habits for Managing the Switch 24

Chapter 2
Tutorials **25**

2.1 How to Use DHCP Snooping on the Switch 25
2.2 How to Use DHCP Relay on the Switch 28
2.2.1 DHCP Relay Tutorial Introduction 29
2.2.2 Creating a VLAN 29
2.2.3 Configuring DHCP Relay 32
2.2.4 Troubleshooting 33
2.3 How to Use PPPoE IA on the Switch 33
2.3.1 Configuring Switch A 34
2.3.2 Configuring Switch B 36
2.4 How to Use Error Disable and Recovery on the Switch 38
2.5 Creating a VLAN 40
2.6 Setting Port VID 41
2.7 How to Set Up a Guest VLAN 42
2.7.1 Creating a Guest VLAN 42
2.7.2 Enabling IEEE 802.1x Port Authentication 45
2.7.3 Enabling Guest VLAN 46

Chapter 3
Switch Hardware Overview 49

3.1 Front Panel Connections 49
3.1.1 (Q)SFP+ Transceiver Slots 49
3.2 Rear Panel 51
3.2.1 Power Connection 51
3.3 Switch LEDs 52

Chapter 4
The Web Configurator 53

4.1 Introduction 53
4.2 System Login 53
4.3 The Web Configurator Layout 54
4.3.1 Change Your Password 58
4.4 Saving Your Configuration 59
4.5 Switch Lockout 59
4.6 Resetting the Switch 59
4.6.1 Reload the Configuration File 59
4.7 Logging Out of the Web Configurator 61
4.8 Help 61

Part II: Technical Reference 63

Chapter 5
System Status and Port Statistics 65

5.1 Overview 65
5.2 Port Status Summary 65
5.2.1 Status: Port Details 66

Chapter 6
Basic Setting 70

6.1 Overview 70
6.2 System Information 70
6.3 General Setup 72
6.4 Introduction to VLANs 73
6.5 Switch Setup Screen 74
6.6 IP Setup 76
6.7 Port Setup 78
6.7.1 Auto-negotiation 78

Chapter 7
VLAN 81

7.1 Introduction to IEEE 802.1Q Tagged VLANs 81
7.1.1 Forwarding Tagged and Untagged Frames 81
7.2 Automatic VLAN Registration 82
7.2.1 GARP 82
7.2.2 GVRP 82
7.3 Port VLAN Trunking 83
7.4 Select the VLAN Type 83
7.5 802.1Q Static VLAN 83
7.5.1 VLAN Status 84
7.5.2 VLAN Details 85
7.5.3 Configure a Static VLAN or Private VLAN 86
7.5.4 Configure VLAN Port Settings 88
7.5.5 Subnet Based VLANs 89
7.5.6 Protocol Based VLANs 91
7.5.7 View Private VLAN Status 94
7.6 Port-based VLAN Setup 95
7.6.1 Configure a Port-based VLAN 95

Chapter 8
Static MAC Forward Setup 99

8.1 Overview 99
8.2 Configuring Static MAC Forwarding 99

Chapter 9
Static Multicast Forward Setup 101

9.1 Static Multicast Forwarding Overview 101
9.2 Configuring Static Multicast Forwarding 102

Chapter 10
Filtering 105

10.1 Configure a Filtering Rule 105

Chapter 11
Spanning Tree Protocol 107

11.1 STP/RSTP Overview 107
11.1.1 STP Terminology 107
11.1.2 How STP Works 108
11.1.3 STP Port States 108
11.1.4 Multiple RSTP 108
11.1.5 Multiple STP 109
11.2 Spanning Tree Protocol Status Screen 112
11.3 Spanning Tree Configuration 112
11.4 Configure Rapid Spanning Tree Protocol 113

11.5 Rapid Spanning Tree Protocol Status 114
11.6 Configure Multiple Rapid Spanning Tree Protocol 116
11.7 Multiple Rapid Spanning Tree Protocol Status 117
11.8 Configure Multiple Spanning Tree Protocol 119
11.8.1 Multiple Spanning Tree Protocol Port Configuration 122
11.9 Multiple Spanning Tree Protocol Status 123

Chapter 12
Bandwidth Control 125

12.1 Bandwidth Control Overview 125
12.1.1 CIR and PIR 125
12.2 Bandwidth Control Setup 126

Chapter 13
Broadcast Storm Control 128

13.1 Broadcast Storm Control Setup 128

Chapter 14
Mirroring 130

14.1 Port Mirroring Setup 130

Chapter 15
Link Aggregation 132

15.1 Link Aggregation Overview 132
15.2 Dynamic Link Aggregation 132
15.2.1 Link Aggregation ID 133
15.3 Link Aggregation Status 133
15.4 Link Aggregation Setting 135
15.5 Link Aggregation Control Protocol 137
15.6 Static Trunking Example 138

Chapter 16
Port Authentication 140

16.1 Port Authentication Overview 140
16.1.1 IEEE 802.1x Authentication 140
16.1.2 MAC Authentication 141
16.2 Port Authentication Configuration 142
16.2.1 Activate IEEE 802.1x Security 143
16.2.2 Guest VLAN 144
16.2.3 Activate MAC Authentication 146

Chapter 17
Port Security 148

17.1 About Port Security 148
17.2 Port Security Setup 148
17.3 VLAN MAC Address Limit 150

Chapter 18
Classifier 151

18.1 About the Classifier and QoS 151
18.2 Configuring the Classifier 151
18.3 Viewing and Editing Classifier Configuration 154
18.4 Classifier Example 156

Chapter 19
Policy Rule 157

19.1 Policy Rules Overview 157
19.1.1 DiffServ 157
19.1.2 DSCP and Per-Hop Behavior 157
19.2 Configuring Policy Rules 157
19.3 Viewing and Editing Policy Configuration 160
19.4 Policy Example 161

Chapter 20
Queuing Method 162

20.1 Queuing Method Overview 162
20.1.1 Strictly Priority Queuing 162
20.1.2 Weighted Fair Queuing 162
20.1.3 Weighted Round Robin Scheduling (WRR) 163
20.2 Configuring Queuing 163

Chapter 21
VLAN Stacking 165

21.1 VLAN Stacking Overview 165
21.1.1 VLAN Stacking Example 165
21.2 VLAN Stacking Port Roles 166
21.3 VLAN Tag Format 167
21.3.1 Frame Format 167
21.4 Configuring VLAN Stacking 168
21.4.1 Port-based Q-in-Q 169
21.4.2 Selective Q-in-Q 170

Chapter 22
Multicast 172

22.1 Multicast Overview 172
22.1.1 IP Multicast Addresses 172

22.1.2 IGMP Filtering 172
22.1.3 IGMP Snooping 172
22.1.4 IGMP Snooping and VLANs 173
22.2 Multicast Status 173
22.3 Multicast Setting 174
22.4 IGMP Snooping VLAN 177
22.5 IGMP Filtering Profile 178
22.6 MVR Overview 179
22.6.1 Types of MVR Ports 180
22.6.2 MVR Modes 180
22.6.3 How MVR Works 180
22.7 General MVR Configuration 181
22.8 MVR Group Configuration 183
22.8.1 MVR Configuration Example 184

Chapter 23
AAA 187

23.1 Authentication, Authorization and Accounting (AAA) 187
23.1.1 Local User Accounts 187
23.1.2 RADIUS and TACACS+ 188
23.2 AAA Screens 188
23.2.1 RADIUS Server Setup 188
23.2.2 TACACS+ Server Setup 191
23.2.3 AAA Setup 193
23.2.4 Vendor Specific Attribute 195
23.2.5 Tunnel Protocol Attribute 196
23.3 Supported RADIUS Attributes 196
23.3.1 Attributes Used for Authentication 197
23.3.2 Attributes Used for Accounting 197

Chapter 24
IP Source Guard 200

24.1 IP Source Guard Overview 200
24.1.1 IP Source Guard Menu Overview 201
24.1.2 DHCP Snooping Overview 201
24.1.3 ARP Inspection Overview 203
24.2 IP Source Guard 204
24.3 Static Binding 205
24.4 DHCP Snooping 207
24.5 DHCP Snooping Configure 209
24.5.1 DHCP Snooping Port Configure 211
24.5.2 DHCP Snooping VLAN Configure 212
24.6 ARP Inspection 213

24.6.1 ARP Inspection VLAN Status 214
24.6.2 ARP Inspection Log Status 215
24.7 ARP Inspection Configure 216
24.7.1 ARP Inspection Port Configure 217
24.7.2 ARP Inspection VLAN Configure 219

Chapter 25
Loop Guard 220

25.1 Loop Guard Overview 220
25.2 Loop Guard Setup 222

Chapter 26
VLAN Mapping 224

26.1 VLAN Mapping Overview 224
26.1.1 VLAN Mapping Example 224
26.2 Enabling VLAN Mapping 225
26.3 Configuring VLAN Mapping 226

Chapter 27
Layer 2 Protocol Tunneling 228

27.1 Layer 2 Protocol Tunneling Overview 228
27.1.1 Layer-2 Protocol Tunneling Mode 229
27.2 Configuring Layer 2 Protocol Tunneling 230

Chapter 28
sFlow 232

28.1 sFlow Overview 232
28.2 sFlow Port Configuration 233
28.2.1 sFlow Collector Configuration 234

Chapter 29
PPPoE 236

29.1 PPPoE Intermediate Agent Overview 236
29.1.1 PPPoE Intermediate Agent Tag Format 236
29.1.2 Sub-Option Format 236
29.1.3 Port State 237
29.2 The PPPoE Screen 238
29.3 PPPoE Intermediate Agent 238
29.3.1 PPPoE IA Per-Port 240
29.3.2 PPPoE IA Per-Port Per-VLAN 241
29.3.3 PPPoE IA for VLAN 243

Chapter 30
Error Disable 244

30.1 CPU Protection Overview 244
30.2 Error-Disable Recovery Overview 244
30.3 The Error Disable Screen 245
30.4 CPU Protection Configuration 245
30.5 Error-Disable Detect Configuration 246
30.6 Error-Disable Recovery Configuration 247

Chapter 31
Private VLAN 249

31.1 Private VLAN Overview 249
31.1.1 Configuration 251

Chapter 32
Static Route 253

32.1 Static Routing Overview 253
32.2 Configuring Static Routing 254

Chapter 33
Differentiated Services 256

33.1 DiffServ Overview 256
33.1.1 DSCP and Per-Hop Behavior 256
33.1.2 DiffServ Network Example 256
33.2 Two Rate Three Color Marker Traffic Policing 257
33.2.1 TRTCM - Color-blind Mode 258
33.2.2 TRTCM - Color-aware Mode 258
33.3 Activating DiffServ 258
33.3.1 Configuring 2-Rate 3 Color Marker Settings 259
33.4 DSCP-to-IEEE 802.1p Priority Settings 261
33.4.1 Configuring DSCP Settings 261

Chapter 34
DHCP 263

34.1 DHCP Overview 263
34.1.1 DHCP Configuration Options 263
34.2 DHCP Status 263
34.3 DHCP Relay 264
34.3.1 DHCP Relay Agent Information 264
34.3.2 Configuring DHCP Global Relay 265
34.3.3 Global DHCP Relay Configuration Example 266
34.4 Configuring DHCP VLAN Settings 266
34.4.1 Example: DHCP Relay for Two VLANs 267

Chapter 35
Maintenance 269

35.1 The Maintenance Screen 269
35.2 Load Factory Default 270
35.3 Save Configuration 270
35.4 Reboot System 270
35.5 Firmware Upgrade 271
35.6 Restore a Configuration File 272
35.7 Backup a Configuration File 272
35.8 FTP Command Line 273
35.8.1 Filename Conventions 273
35.8.2 FTP Command Line Procedure 274
35.8.3 GUI-based FTP Clients 274
35.8.4 FTP Restrictions 274

Chapter 36
Access Control 276

36.1 Access Control Overview 276
36.2 The Access Control Main Screen 276
36.3 About SNMP 276
36.3.1 SNMP v3 and Security 277
36.3.2 Supported MIBs 278
36.3.3 SNMP Traps 278
36.3.4 Configuring SNMP 282
36.3.5 Configuring SNMP Trap Group 283
36.3.6 Configuring SNMP User 284
36.4 Setting Up Login Accounts 285
36.5 Service Access Control Overview 287
36.5.1 SSH 287
36.5.2 HTTPS 288
36.5.3 Configuring Service Port Access Control 293
36.6 Remote Management 294

Chapter 37
Diagnostic 296

37.1 Diagnostic 296

Chapter 38
Syslog 297

38.1 Syslog Overview 297
38.2 Syslog Setup 298
38.3 Syslog Server Setup 299

Chapter 39
Cluster Management 300

39.1 Clustering Management Status Overview 300
39.2 Cluster Management Status 301
39.2.1 Cluster Member Switch Management 302
39.3 Clustering Management Configuration 304

Chapter 40
MAC Table 306

40.1 MAC Table Overview 306
40.2 Viewing the MAC Table 307

Chapter 41
ARP Table 309

41.1 ARP Table Overview 309
41.1.1 How ARP Works 309
41.2 The ARP Table Screen 310

Chapter 42
Configure Clone 311

42.1 Configure Clone 311

Chapter 43
Troubleshooting 313

43.1 Power, Hardware Connections, and LEDs 313
43.2 Switch Access and Login 314
43.3 Switch Configuration 316

Appendix A Common Services 317

Appendix B Legal Information 321

Index 323

PART I
User's Guide

1

Getting to Know Your Switch

This chapter introduces the main features and applications of the Switch.

1.1 Introduction

This is a high-speed, layer-2, enhanced Ethernet switch with FCoE (Fiber Channel over Ethernet) and DCB (Data Center Bridging) features.

The Switch comes with:

- Forty-eight 10GbE SFP+ ports and four 40GbE QSFP+ ports at the front
- Two power slots for power modules and two slots for fan modules at the back. The power and fan modules are hot-swappable and you can choose between front-to-rear and rear-to-front airflow depending on your installation.

Other key features include SNMP, STP, VLAN, QinQ, Trunk, QoS, and Access Control.

With its built-in web configurator, managing and configuring the Switch is easy. In addition, the Switch can also be managed via Telnet, any terminal emulator program on the console port, or third-party SNMP management.

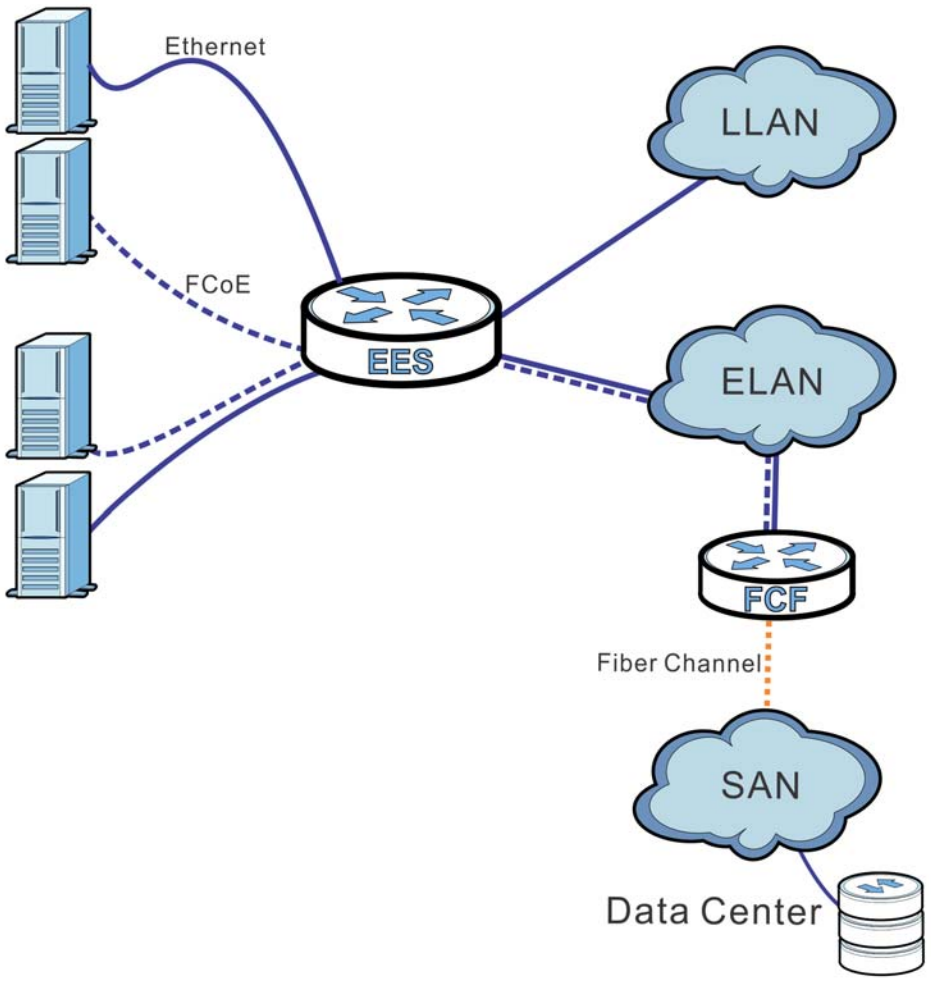
See the datasheet for a full list of software features available on this Switch.

1.2 Data Center Bridging (DCB)

A traditional Ethernet network is best-effort, that is, frames may be dropped due to device queue overflow or network congestion. FCoE (Fiber Channel over Ethernet) transparently encapsulates fiber channel traffic into Ethernet, so that you don't need separate fiber channel and Ethernet switches.

Data Center Bridging (DCB) enhances Ethernet technology to adapt to the FCoE. It supports lossless Ethernet traffic (no frames discarded when there is network congestion) and can allocate bandwidth for different traffic classes, based on IEEE802.1p priority with a guaranteed minimum bandwidth. LAN traffic (large number of flows and not latency-sensitive), SAN traffic (Storage Area Network, large packet sizes and requires lossless performance), and IPC traffic (Inter-Process Communication, latency-sensitive messages) can share the same physical connection while still having its own priority and guaranteed minimum bandwidth.

The following figure shows an example deployment for the Switch using DCB.



The following table explains the acronyms in the graphic.

Table 1 DCB Graphic Key

LABEL	DESCRIPTION
EES	Enhanced Ethernet Switch
LLAN	Legacy Local Area Network (Ethernet)
ELAN	Enhanced LAN (Ethernet & FCoE)
FCF	Fiber Channel Forwarder
SAN	Storage Access Network

1.2.1 PFC, ETS, and DCBX Standards

DCB may use PFC, ETS, application priority and DCBX to adapt to the FCoE.

- PFC (Priority-based Flow Control, IEEE 802.1Qbb -2011) is a flow control mechanism that uses a PAUSE frame to suspend traffic of a certain priority rather than drop it when there is network congestion (lossless). If an outgoing (egress) port buffer is almost full, the Switch transmits a PAUSE frame to the sender who just transmitted traffic requesting it to stop sending traffic of a certain priority to that port. For example, say outgoing port 8 is receiving too much traffic of priorities 3-6 from port 1. Then if port 1 is configured with PFC priorities 3-6, port 1 can request the sender to suspend traffic with priorities 3-6.

  Similarly, if the outcoming (egress) port 8 receives a PAUSE frame with PFC priorities 0-1, then if port 8 is configured with PFC, it can suspend sending traffic with PFC priorities 0-1.
- ETS (Enhanced Transmission Selection, IEEE 802.1Qaz -2011) is used to allocate bandwidth for different traffic classes, based on IEEE802.1p priority (0 to 7, allowing for eight types of traffic) with a guaranteed minimum bandwidth.
- Application priority is used to globally assign a priority to all FCoE traffic on the Switch.
- DCBX (Data Center Bridging capability eXchange, IEEE 802.1Qaz -2011) uses LLDP (Link Layer Discovery Protocol) to advertize PFC, ETS and application priority information between switches. PFC information should be consistent between connected switches, so PFC can be configured automatically using DCBX.

1.2.2 DCB Configuration

You should configure DCB on any port that has both Ethernet and FCoE traffic.

1.2.2.1 DCB Only

Do the following if you're just using DCB, that is, switches don't need to know DCB-related configurations via DCBX.

ETS

- Configure ETS to define traffic classes based on priority. Assign a weighted guaranteed bandwidth for non strict priority (SP) traffic. SP traffic always has first priority.

  First, define traffic classes. This is an example where the non-editable default traffic class, ID 0, uses SP queuing. LAN and SAN traffic uses WFQ queuing with equal weighting of 50 each.

Table 2 Defined Traffic Classes

TRAFFIC CLASS ID	GUARANTEED BANDWIDTH	CLASS NAME
0	SP	Default
1	50	SAN
2	50	LAN

Next, define relative weights for non-SP traffic. In the example, the guaranteed minimum bandwidth for both SAN and LAN traffic is 2.5Gbp with a physical link bandwidth of 10Gbps.

Table 3 Defined Relative Weights

NAME	INCOMING TRAFFIC BANDWIDTH (GBPS)	GUARANTEED MINIMUM BANDWIDTH	OUTGOING TRAFFIC BANDWIDTH (GBPS)
Default	5	5 (SP)	5
SAN	3	(10-5) * (50/(50+50)) = 2.5	2.5
LAN	4	(10-5) * (50/(50+50)) = 2.5	2.5

Next, configure port 1 and bind priorities as follows:

- 0, 1 and 2 to traffic class 2 (LAN)
- 3, 4, 5 and 6 to ID 1 (SAN)
- 7 to 0, the default traffic class.

If there is network congestion, bandwidth can be allocated based on the priority of the traffic received on that port.

Table 4 Bound Traffic Priorities

PRIORITY	TRAFFIC CLASS ID	NAME
0	2	LAN
1	2	LAN
2	2	LAN
3	1	SAN
4	1	SAN
5	1	SAN
6	1	SAN
7	0	Default

PFC

- Estimate what traffic types are likely to cause network congestion and configure PFC with these associated priorities. For example, if SAN traffic is likely to cause congestion, then configure PFC with priorities 3, 4, 5, 6. It's better if the connected peer switch has the same configured priorities.

1.2.2.2 DCB with DCBX

Do the following if you're using DCB with DCBX, that is, switches need to know each other's PFC, ETS and application priority information.

- Enable transmission and reception of LLDP PDUs (Protocol Data Unit) on a port using `lldp admin-status tx-rx`.
- Enable TLV (Type-Length-Value) transmission of formats so that switches can read each others ETS, PFC and application priority information sent via LLDP PDUs.
- Configure ETS as outlined in the previous section.
- Configure application priority for all FCoE traffic on the Switch.

- Set PFC to auto (Willing = True) if you want the Switch to accept PFC priority configuration from another switch. In the following example, switch A sends its LLDP PDU with PFC TLV, local priorities 3, 4, 5 and auto (Willing field is set to true, meaning it is willing to accept PFC priorities from the peer). Switch B's local priorities are 0 and 1 and Willing field is set to false, meaning it is not willing to accept PFC priorities from the peer, switch A). Switch A will use switch B's configured priorities 0 and 1.

Switch A LLDP PDU			**Switch B LLDP PDU**		
PFC TLV	3,4,5	Willing = True			
			PFC TLV	0,1	Willing = False
PFC TLV	0,1	Willing = True			

  If both switches are configured to accept configuration (auto on both switches), then the configuration of the switch with the lowest MAC address hex value sum is used.

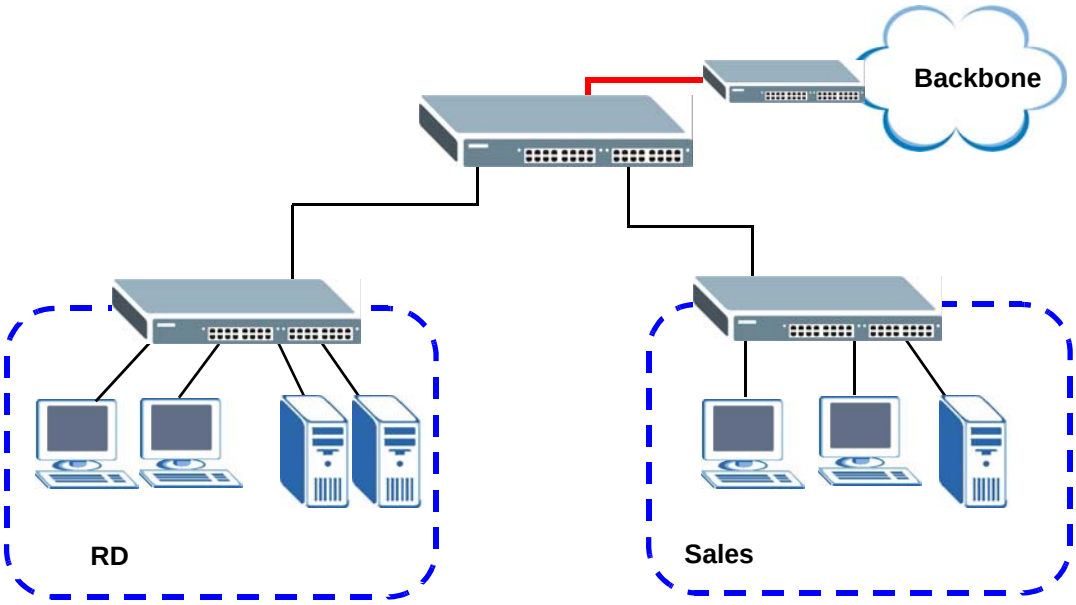
- Verify configurations by displaying all port and Switch (local and peer) LLDP information. Local port and Switch configuration and statistics can also be viewed.

Note: At the time of writing, DCB is configured using the Command Line Interface (CLI) only. See the CLI reference guide for details and usage examples.

1.3 Bridging Example

In this example the Switch connects different company departments (**RD** and **Sales**) to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the Switch. You can provide a super-fast uplink connection by using the optional 10 Gigabit uplink module on the Switch.

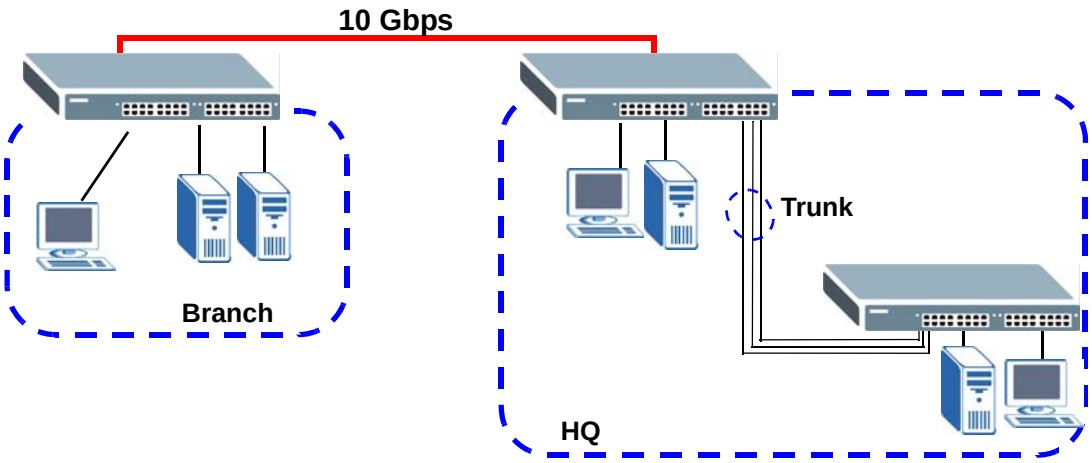
Figure 1 Bridging Application



1.4 High Performance Switching Example

The Switch is ideal for connecting two geographically dispersed networks that need high bandwidth. In the following example, a company uses the optional 10 Gigabit uplink modules to connect the headquarters to a branch office network. Within the headquarters network, a company can use trunking to group several physical ports into one logical higher-capacity link. Trunking can be used if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

Figure 2 High Performance Switching



1.5 IEEE 802.1Q VLAN Application Example

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one or more groups. With VLAN, a station cannot directly talk to or hear from stations that are not in the same group(s) unless such traffic first goes through a router.

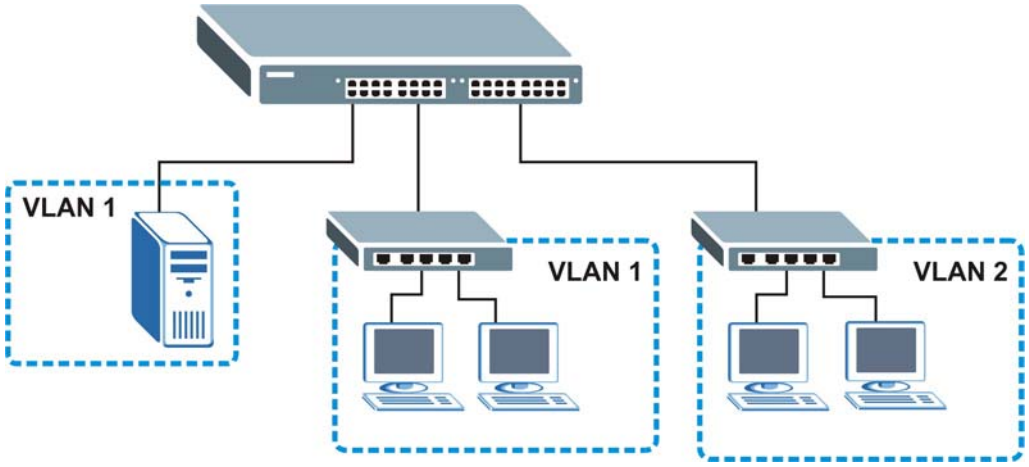
For more information on VLANs, refer to Chapter 7 on page 81.

1.5.0.1 Tag-based VLAN Example

Ports in the same VLAN group share the same frame broadcast domain, thus increasing network performance by reducing broadcast traffic. VLAN groups can be modified at any time by adding, moving or changing ports without any re-cabling.

Shared resources such as a server can be used by all ports in the same VLAN as the server. In the following figure only ports that need access to the server need to be part of VLAN 1. Ports can belong to other VLAN groups too.

Figure 3 Shared Server Using VLAN Example



1.6 IPv6 Support

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4 x 10^{38} IP addresses. At the time of writing, the Switch supports the following features.

- Static address assignment and stateless auto-configuration
- Neighbor Discovery Protocol (a protocol used to discover other IPv6 devices in a network)
- Remote Management using ping SNMP, telnet, HTTP and FTP services
- ICMPv6 to report errors encountered in packet processing and perform diagnostic functions, such as "ping"
- IPv4/IPv6 dual stack; the Switch can run IPv4 and IPv6 at the same time
- DHCPv6 client and relay
- Multicast Listener Discovery (MLD) snooping and proxy
- For more information on IPv6, refer to the CLI Reference Guide.

1.7 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- Web Configurator. This is recommended for everyday management of the Switch using a (supported) web browser. See Chapter 4 on page 53.
- Command Line Interface. Line commands offer an alternative to the Web Configurator and may be necessary to configure advanced features. See the CLI Reference Guide.
- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup/restore. See Section 35.8 on page 273.

- SNMP. The device can be monitored and/or managed by an SNMP manager. See Section 36.3 on page 276.

1.8 Good Habits for Managing the Switch

Do the following things regularly to make the Switch more secure and to manage the Switch more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the Switch to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the Switch. You could simply restore your last configuration.

2

Tutorials

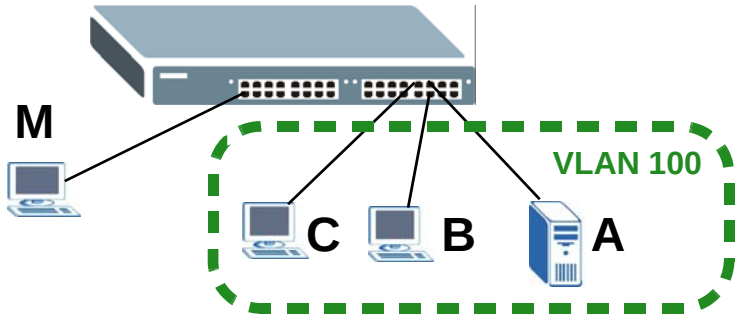
This chapter provides some examples of using the web configurator to set up and use the Switch. The tutorials include:

- How to Use DHCP Snooping on the Switch
- How to Use DHCP Relay on the Switch
- How to Use PPPoE IA on the Switch
- How to Use Error Disable and Recovery on the Switch
- Creating a VLAN
- Setting Port VID
- How to Set Up a Guest VLAN

2.1 How to Use DHCP Snooping on the Switch

You only want DHCP server **A** connected to port 5 to assign IP addresses to all devices in VLAN 100. Create a VLAN containing ports 5, 6 and 7. Connect a computer **M** to the Switch's **MGMT** port.

Figure 4 Tutorial: DHCP Snooping Tutorial Overview



Note: For related information about DHCP snooping, see Section 24.1 on page 200.

The settings in this tutorial are as the following.

Table 5 Settings in this Tutorial

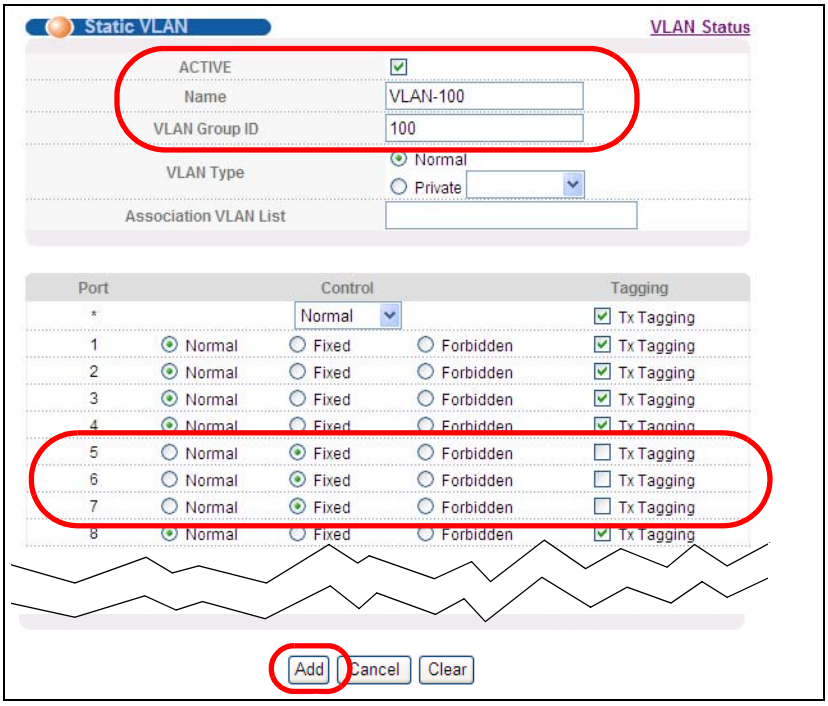
HOST	PORT CONNECTED	VLAN	PVID	DHCP SNOOPING PORT TRUSTED
DHCP Server (**A**)	5	1 and 100	100	Yes
DHCP Client (**B**)	6	1 and 100	100	No
DHCP Client (**C**)	7	1 and 100	100	No

1 Access the Switch from the **MGMT** port through **http://192.168.0.1** by default. Log into the Switch by entering the username (default: **admin**) and password (default: **1234**).

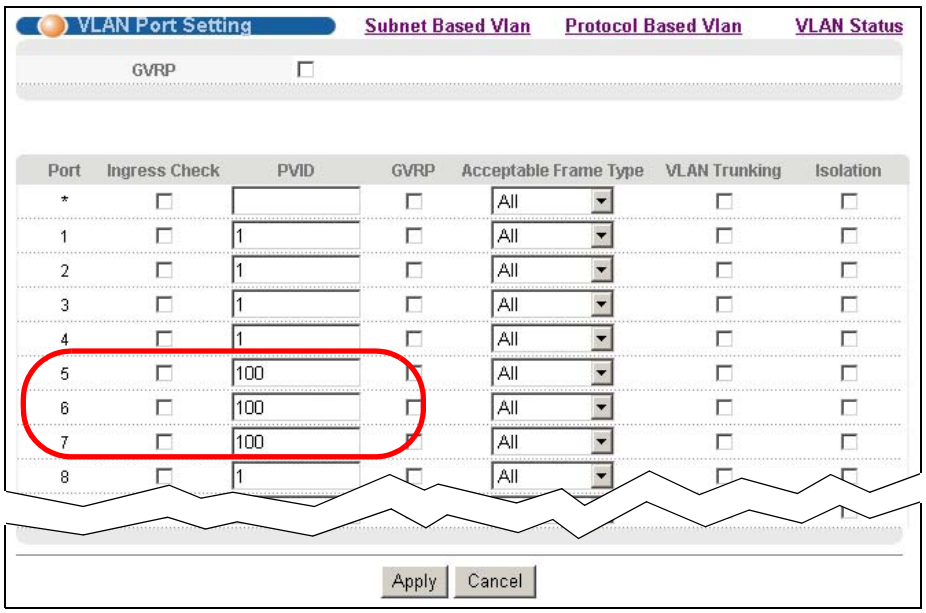
2 Go to **Advanced Application** > **VLAN** > **Static VLAN**, and create a VLAN with ID of 100. Add ports 5, 6 and 7 in the VLAN by selecting **Fixed** in the **Control** field as shown.

Deselect **Tx Tagging** because you don't want outgoing traffic to contain this VLAN tag.

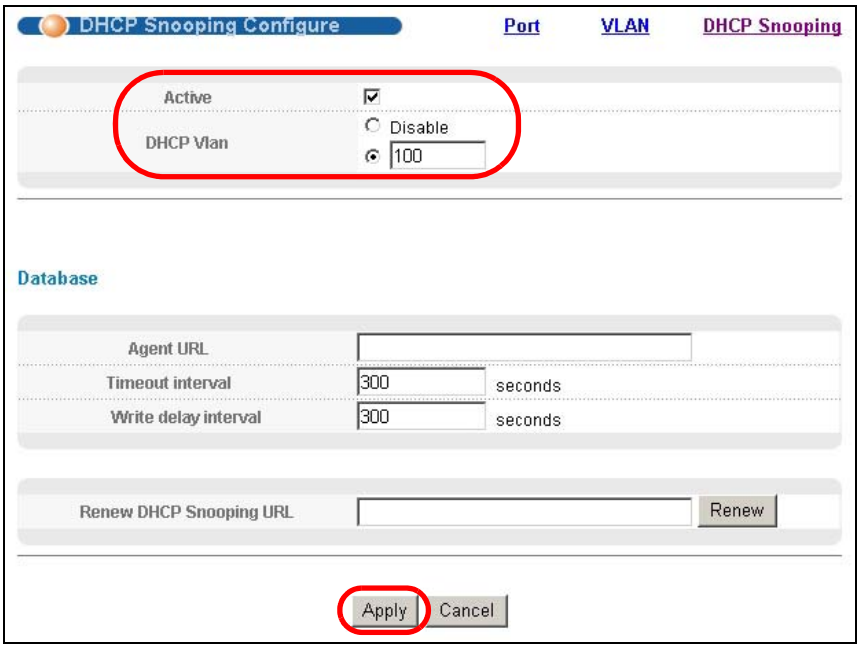
Click **Add**.



3 Go to **Advanced Application** > **VLAN** > **VLAN Port Setting**, and set the PVID of the ports 5, 6 and 7 to 100. This tags untagged incoming frames on ports 5, 6 and 7 with the tag 100.

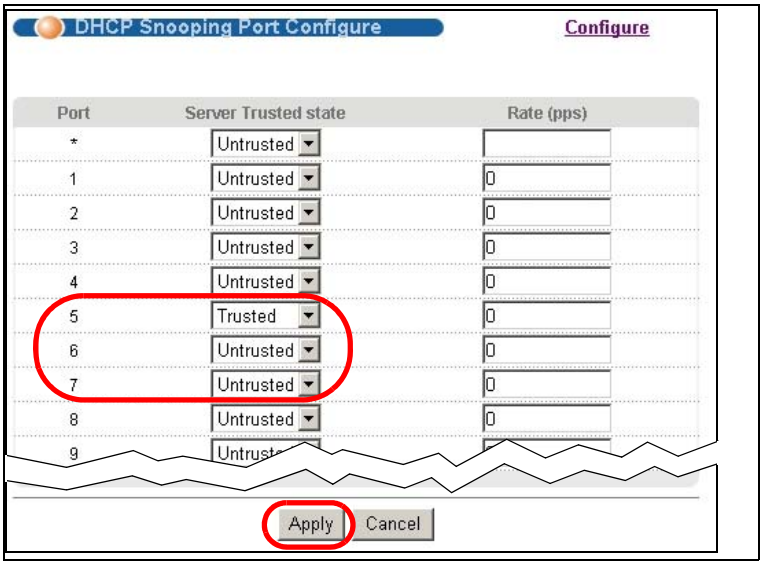


4 Go to **Advanced Application** > **IP Source Guard** > **DHCP snooping** > **Configure**, activate and specify VLAN 100 as the DHCP VLAN as shown. Click **Apply**.



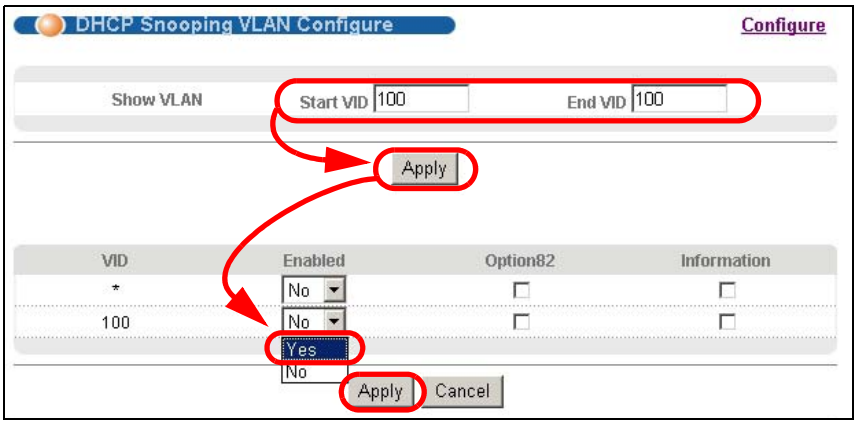
5 Click the **Port** link at the top right corner.

6 The **DHCP Snooping Port Configure** screen appears. Select **Trusted** in the **Server Trusted state** field for port 5 because the DHCP server is connected to port 5. Keep ports 6 and 7 **Untrusted** because they are connected to DHCP clients. Click **Apply**.



7 Go to **Advanced Application** > **IP Source Guard** > **DHCP snooping** > **Configure** > **VLAN**, show VLAN 100 by entering 100 in the **Start VID** and **End VID** fields and click **Apply**. Then select **Yes** in the **Enabled** field of the VLAN 100 entry shown at the bottom section of the screen.

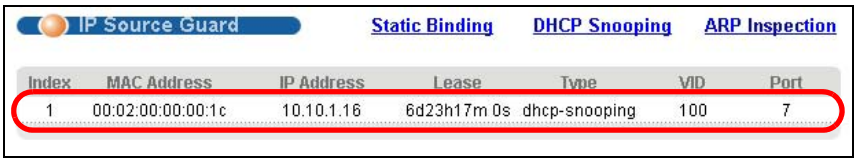
If you want to add more information in the DHCP request packets such as source VLAN ID or system name, you can also select the **Option82** and **Information** fields in the entry. See Section 24.1.2.3 on page 202.



8 Click **Save** at the top right corner of the web configurator to save the configuration permanently.

9 Connect your DHCP server to port 5 and a computer (as DHCP client) to either port 6 or 7. The computer should be able to get an IP address from the DHCP server. If you put the DHCP server on port 6 or 7, the computer will not able to get an IP address.

10 To check if DHCP snooping works, go to **Advanced Application** > **IP Source Guard**, you should see an IP assignment with the type **dhcp-snooping** as shown.



You can also telnet or log into the Switch's console. Use the command "show dhcp snooping binding" to see the DHCP snooping binding table as shown next.

```
sysname# show dhcp snooping binding
         MacAddress        IpAddress         Lease           Type  VLAN   Port
  ----------------  ---------------  ------------  -------------  ----  -----
  00:02:00:00:00:1c       10.10.1.16   6d23h59m20s  dhcp-snooping   100      7
  Total number of bindings: 1
```

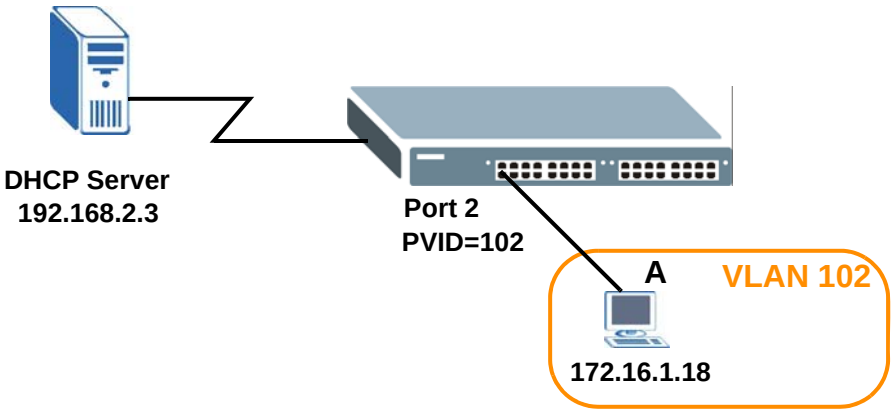
2.2 How to Use DHCP Relay on the Switch

This tutorial describes how to configure your Switch to forward DHCP client requests to a specific DHCP server. The DHCP server can then assign a specific IP address based on the information in the DHCP requests.

2.2.1 DHCP Relay Tutorial Introduction

In this example, you have configured your DHCP server (192.168.2.3) and want to have it assign a specific IP address (say 172.16.1.18) and gateway information to DHCP client **A** based on the system name, VLAN ID and port number in the DHCP request. Client **A** connects to the Switch's port 2 in VLAN 102.

Figure 5 Tutorial: DHCP Relay Scenario

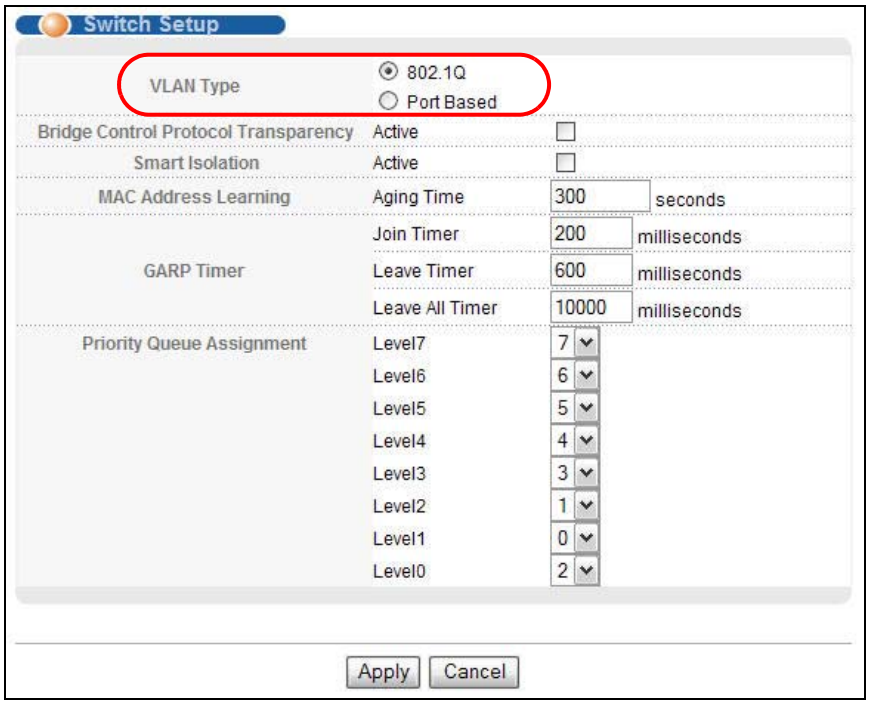


2.2.2 Creating a VLAN

Follow the steps below to configure port 2 as a member of VLAN 102.

1 Access the web configurator through the Switch's management port.

2 Go to **Basic Setting** > **Switch Setup** and set the VLAN type to **802.1Q**. Click **Apply** to save the settings to the run-time memory.



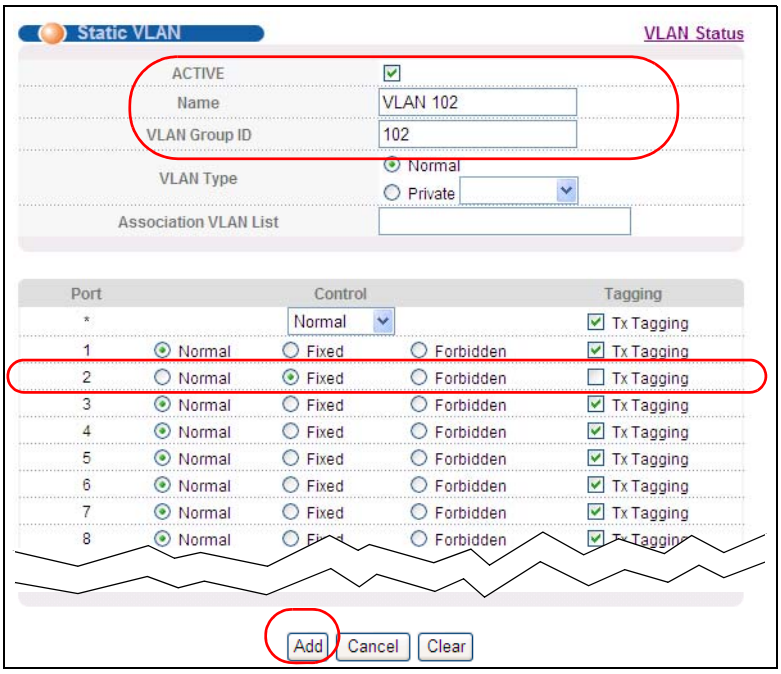
3 Click **Advanced Application** > **VLAN > Static VLAN**.

4 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name (VLAN 102 for example) in the **Name** field and enter 102 in the **VLAN Group ID** field.

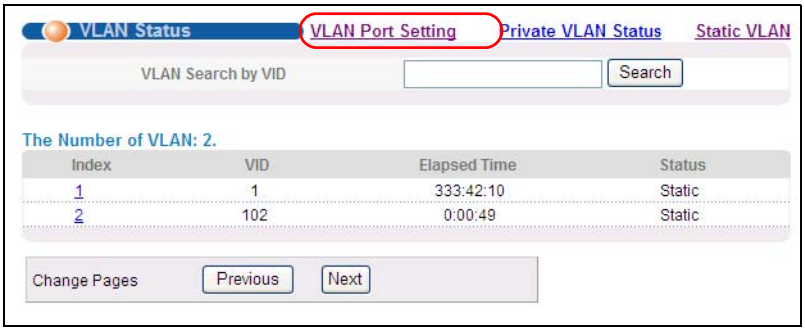
5 Select **Fixed** to configure port 2 to be a permanent member of this VLAN.

6 Clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.

7 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

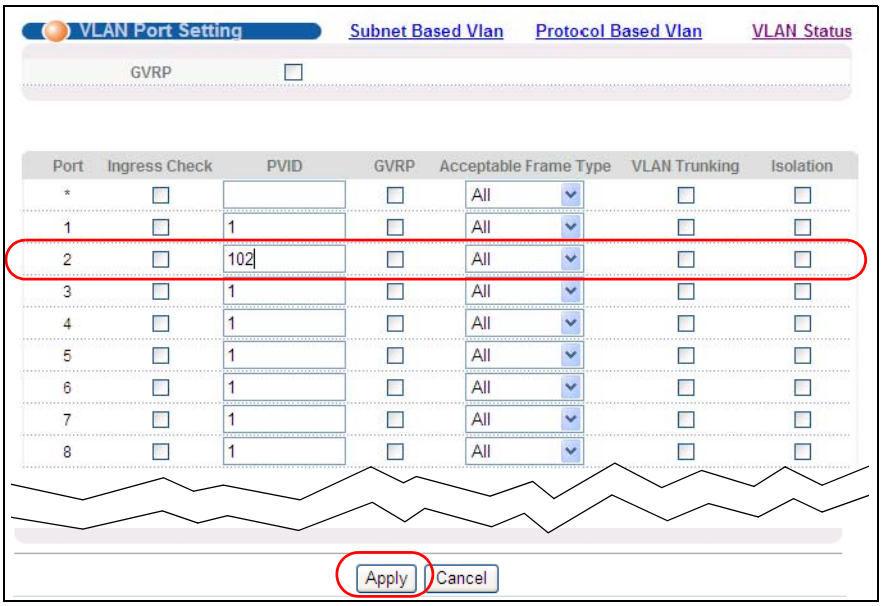


8 Click the **VLAN Status** link in the **Static VLAN** screen and then the **VLAN Port Setting** link in the **VLAN Status** screen.



9 Enter 102 in the **PVID** field for port 2 to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

10 Click **Apply** to save your changes back to the run-time memory.



11 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

2.2.3 Configuring DHCP Relay

Follow the steps below to enable DHCP relay on the Switch and allow the Switch to add relay agent information (such as the VLAN ID) to DHCP requests.

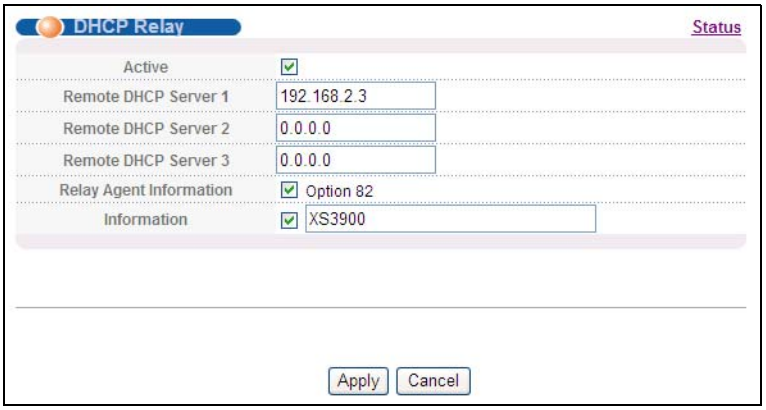
1 Click **IP Application > DHCP** and then the **Global** link to open the **DHCP Relay** screen.

2 Select the **Active** check box.

3 Enter the DHCP server's IP address (192.168.2.3 in this example) in the **Remote DHCP Server 1** field.

4 Select the **Option 82** and the **Information** check boxes.

5 Click **Apply** to save your changes back to the run-time memory.



6 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

7 The DHCP server can then assign a specific IP address based on the DHCP request.

2.2.4 Troubleshooting

Check the client **A**'s IP address. If it did not receive the IP address 172.16.1.18, make sure:

1 Client **A** is connected to the Switch's port 2 in VLAN 102.

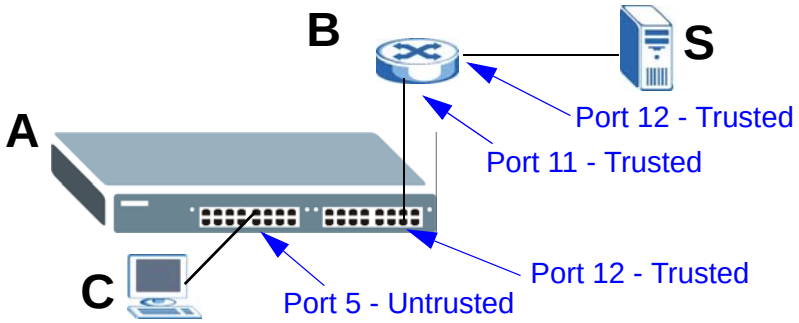
2 You configured the correct VLAN ID, port number and system name for DHCP relay on both the DHCP server and the Switch.

3 You clicked the **Save** link on the Switch to have your settings take effect.

2.3 How to Use PPPoE IA on the Switch

You want to configure PPPoE Intermediate Agent on the Switch (**A**) to pass a subscriber's information to a PPPoE server (**S**). There is another switch (**B**) between switch **A** and server **S**. Switch **B** is connected to switch **A**. In this way, PPPoE server **S** can identify subscriber **C** and may apply different settings to it.

Figure 6 Tutorial: PPPoE Intermediate Agentt Tutorial Overview



Note: For related information about PPPoE IA, see Section 29.3 on page 238.

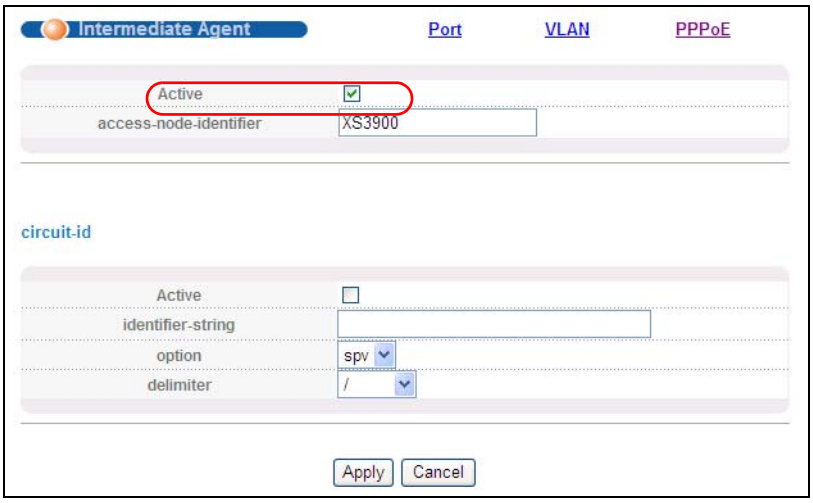
The settings in this tutorial are as follows:

Table 6 Settings in this Tutorial

SWITCH	PORT CONNECTED	VLAN	CIRCUIT-ID	REMOTE-ID	PPPOE IA PORT TRUSTED
A	Port 5 (to **C**)	1	userC	00134900000A	Untrusted
	Port 12 (to **B**)	1	N/A	N/A	Trusted
B	Port 11 (to **A**)	1	N/A	N/A	Trusted
	Port 12 (to **S**)	1	N/A	N/A	Trusted

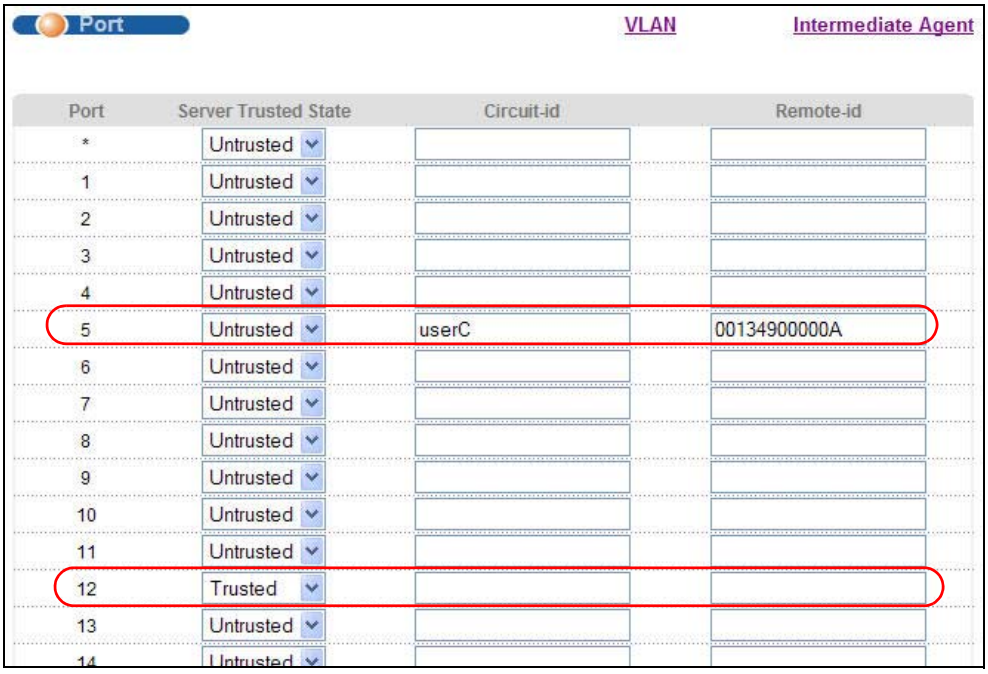
2.3.1 Configuring Switch A

1 Click **Advanced Application > PPPoE > Intermediate Agent**. Select **Active** then click **Apply**.



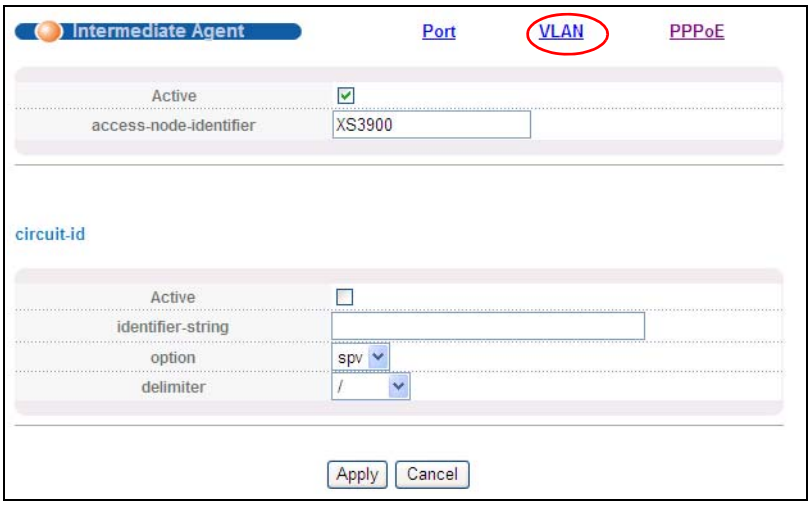
Click **Port** on the top of the screen.

2 Select **Untrusted** for port 5 and enter **userC** as **Circuit-id** and **00134900000A** as **Remote-id**. Select **Trusted** for port 12 and then leave the other fields empty. Click **Apply**.

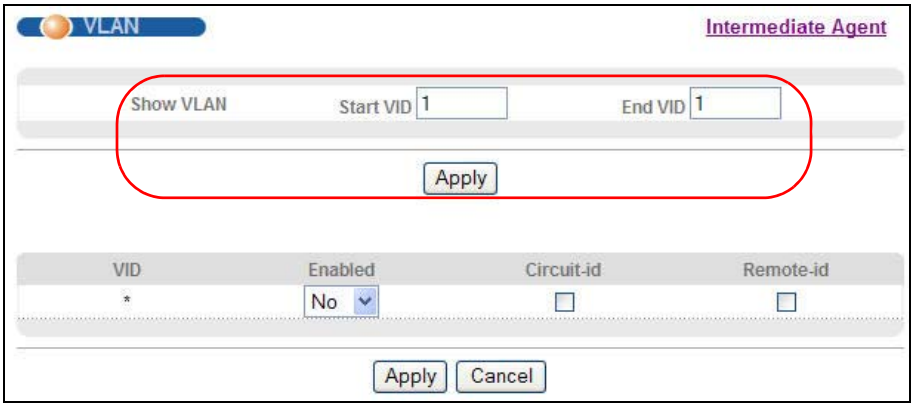


Then Click **Intermediate Agent** on the top of the screen.

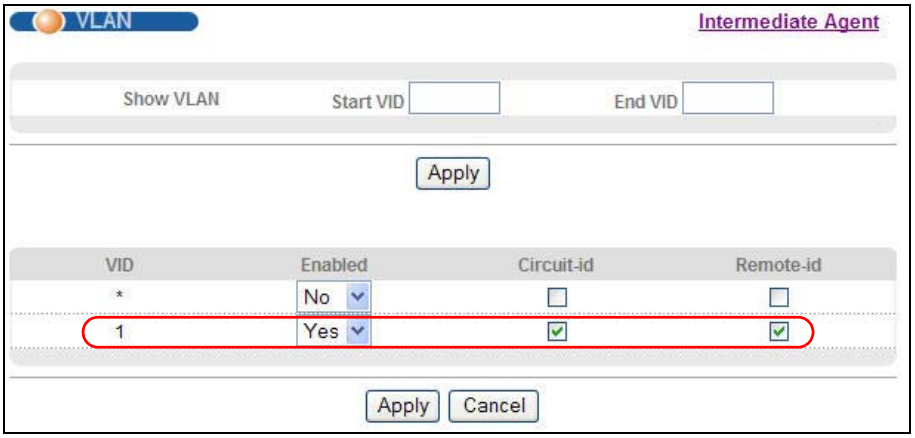
3 The **Intermediate Agent** screen appears. Click **VLAN** on the top of the screen.



4 Enter 1 for both **Start VID** and **End VID** since both the Switch and PPPoE server are in VLAN 1 in this example. Click **Apply**.



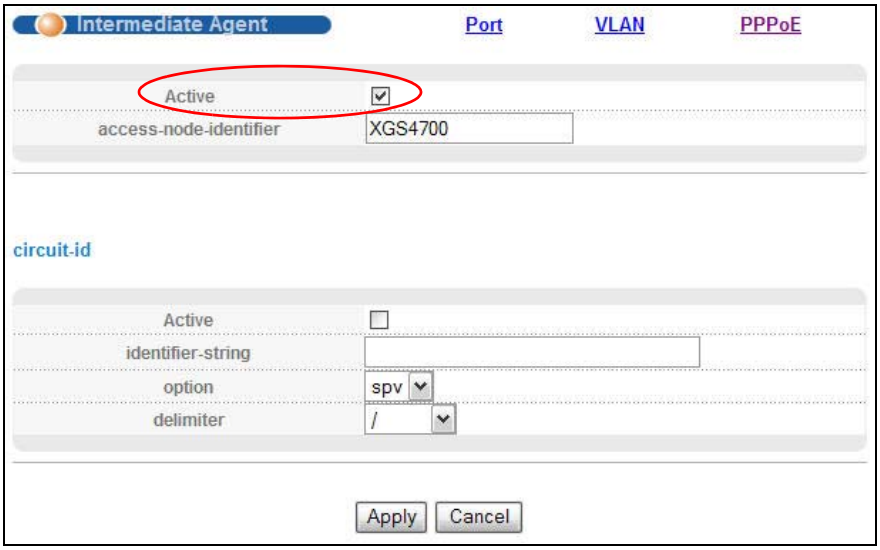
5 Then select **Yes** to enable PPPoE IA in VLAN 1 and also select **Circuit-id** and **Remote-id** to allow the Switch to add these two strings to frames tagged with VLAN 1 and pass to the PPPoE server. Click **Apply**.



2.3.2 Configuring Switch B

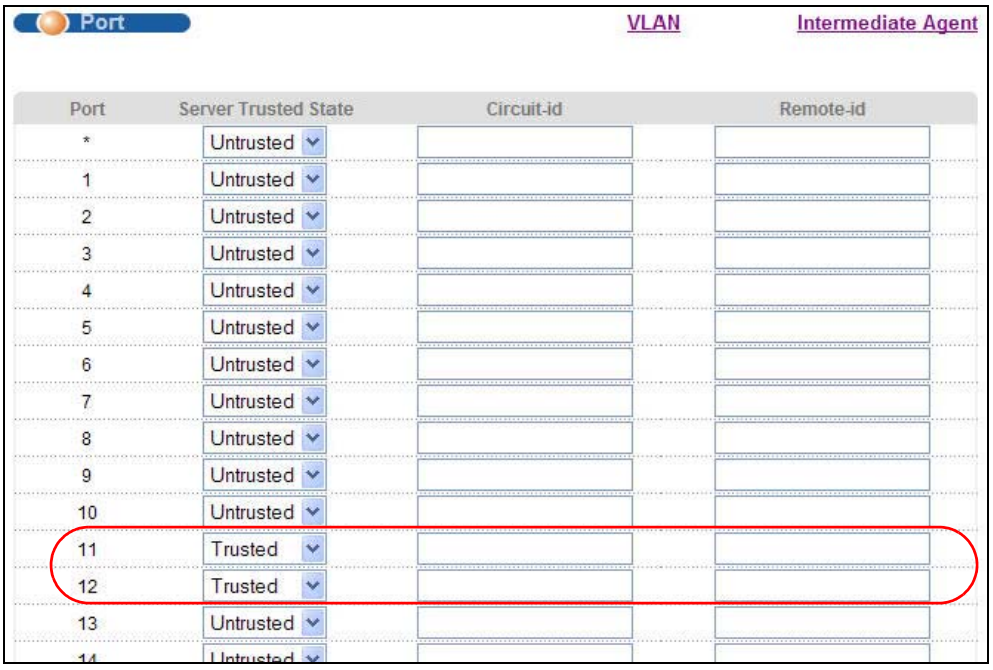
The example uses an XGS4700-48F as switch **B**.

1 Click **Advanced Application > PPPoE > Intermediate Agent**. Select **Active** then click **Apply**.



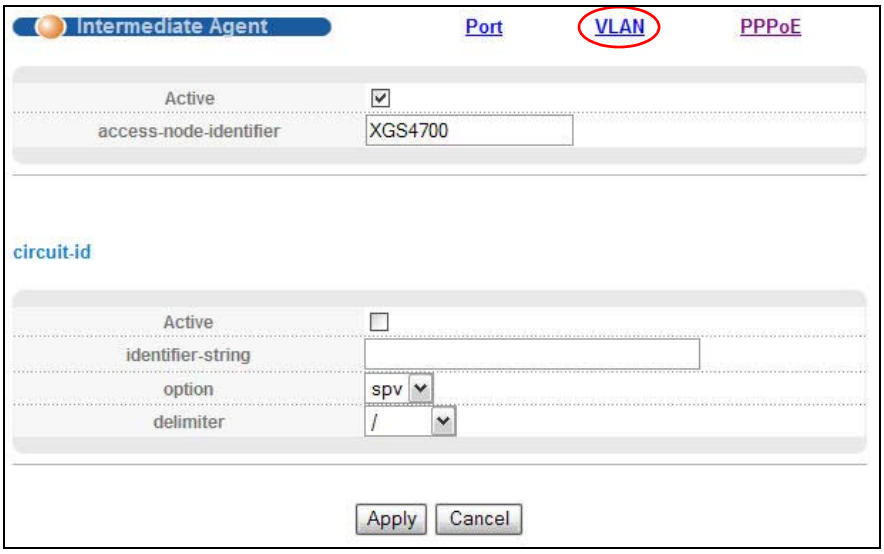
Click **Port** on the top of the screen.

2 Select **Trusted** for ports 11 and 12 and then click **Apply**.

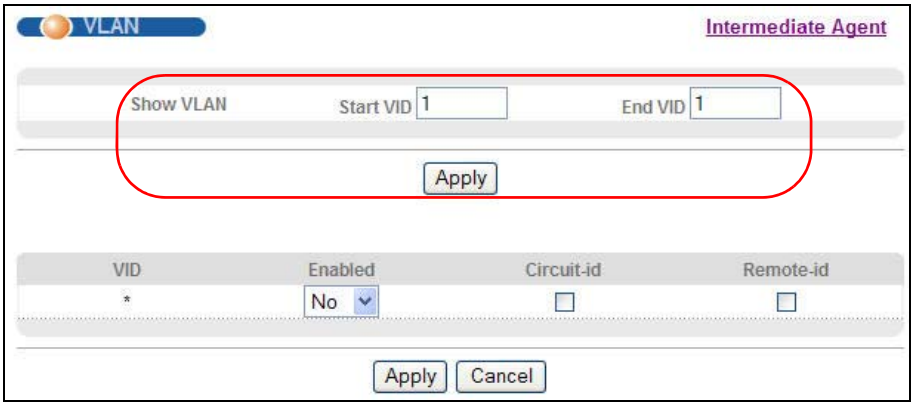


Then Click **Intermediate Agent** on the top of the screen.

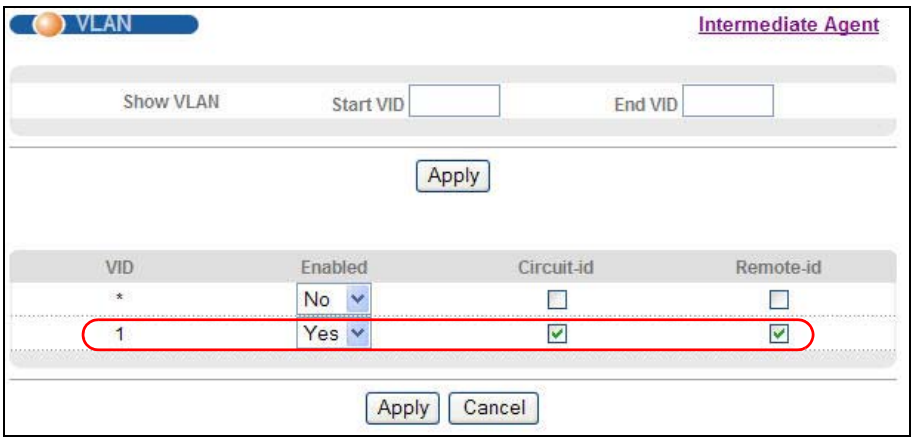
3 The **Intermediate Agent** screen appears. Click **VLAN** on the top of the screen.



4 Enter 1 for both **Start VID** and **End VID**. Click **Apply**.



5 Then select **Yes** to enable PPPoE IA in VLAN 1 and also select **Circuit-id** and **Remote-id** to allow the Switch to add these two strings to frames tagged with VLAN 1 and pass to the PPPoE server. Click **Apply**.



The settings are completed now. If you miss some settings above, subscriber **C** could not successfully receive an IP address assigned by the PPPoE Server. If this happens, make sure you follow the steps exactly in this tutorial.

2.4 How to Use Error Disable and Recovery on the Switch

This tutorial shows you how to shut down a port when:

- a loop has occurred

or

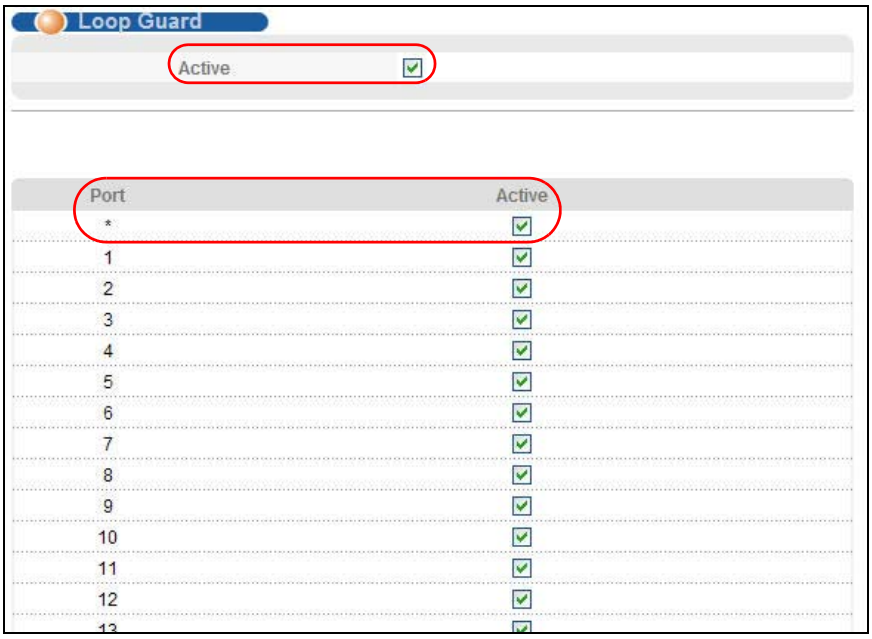
- too many ARP requests (over 100 packets per second) have been received on a port

You also want the Switch to wait for a period of time (10 minutes) before resuming the port automatically, after the problem(s) are gone. Loop guard and Errdiable features are helpful for this demand.

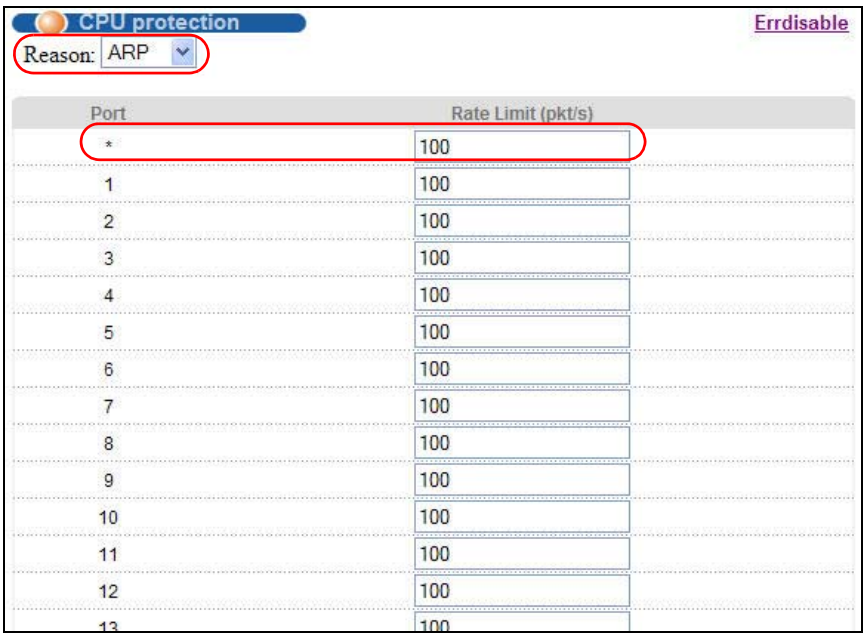
Note: Refer to Section 25.2 on page 222 and Section 30.2 on page 244 for more information about Loop Guard and Errdiable.

To configure the settings:

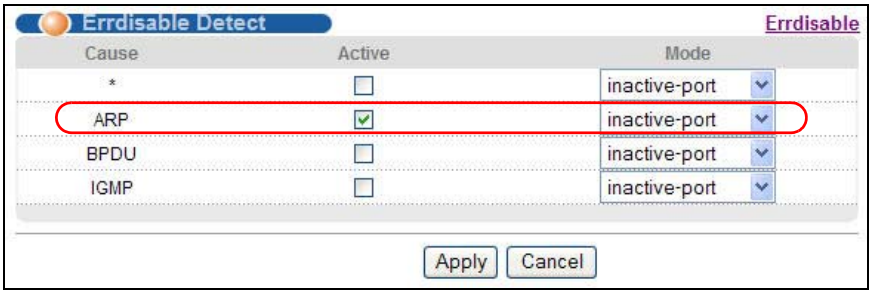
1 First, click **Advanced Application > Loop Guard**. Select the **Active** option in the first section to enable loop guard on the Switch. Then select the **Active** option of the first entry (port *) to enable loop guard for all ports. Click **Apply**.



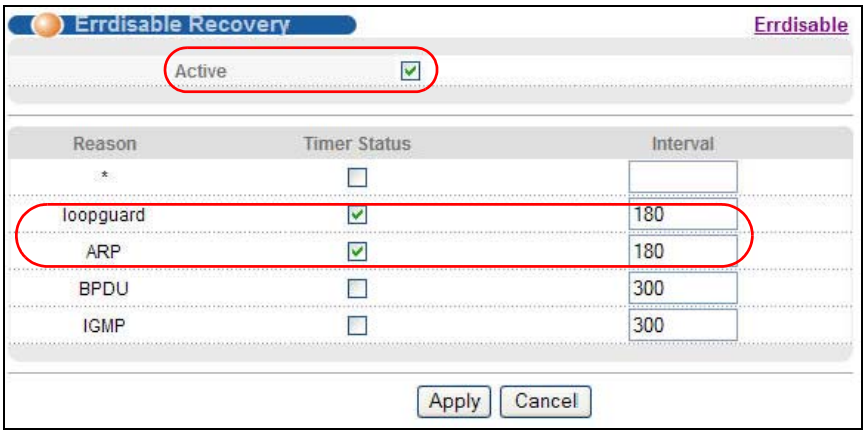
2 Click **Advanced Application > Errdisable > CPU Protection**, select **ARP** as the reason, enter 100 as the rate limit (packets per second) for the first entry (port *) to apply the setting to all ports. Then click **Apply**.



3 Click **Advanced Application > Errdisable > Errdisable Detect**, select **Active** for cause **ARP** and **inactive-port** as the mode. Then click **Apply**.



4 Click **Advanced Application > Errdisable > Errdisable Recovery**, select **Active** and **Timer Status** for **loopguard** and **ARP** entries. Also enter 180 (180 seconds = 3 minutes) in the **Interval** field for both entries. Then click **Apply**.

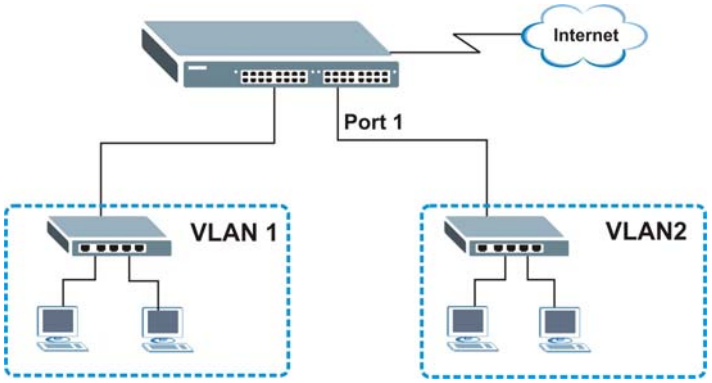


2.5 Creating a VLAN

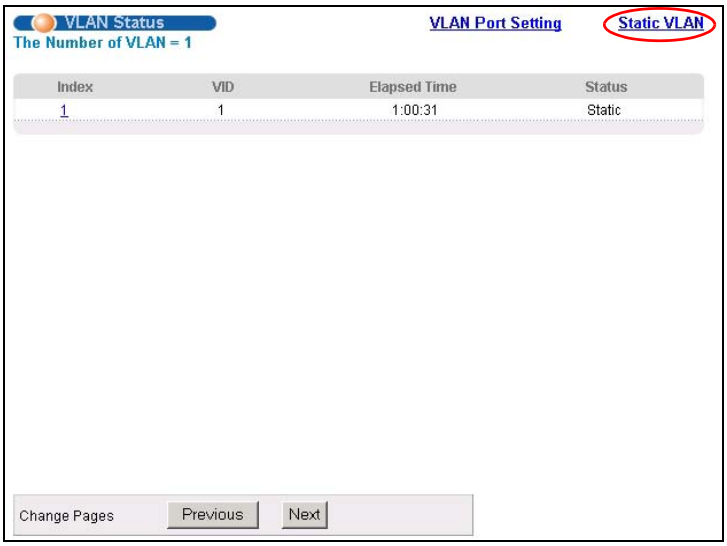
VLANs confine broadcast frames to the VLAN group in which the port(s) belongs. You can do this with port-based VLAN or tagged static VLAN with fixed port members.

In this example, you want to configure port 1 as a member of VLAN 2.

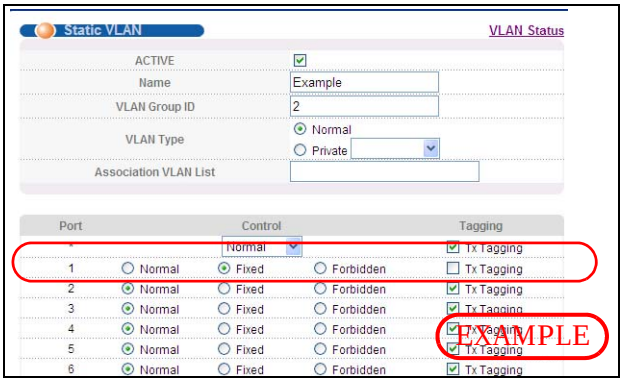
Figure 7 Initial Setup Network Example: VLAN



1 Click **Advanced Application** > **VLAN** in the navigation panel and click the **Static VLAN** link.



2 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name in the **Name** field and enter 2 in the **VLAN Group ID** field for the **VLAN2** network.



Note: The **VLAN Group ID** field in this screen and the **VID** field in the **IP Setup** screen refer to the same VLAN ID.

3 Since the **VLAN2** network is connected to port 1 on the Switch, select **Fixed** to configure port 1 to be a permanent member of the VLAN only.

4 To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.

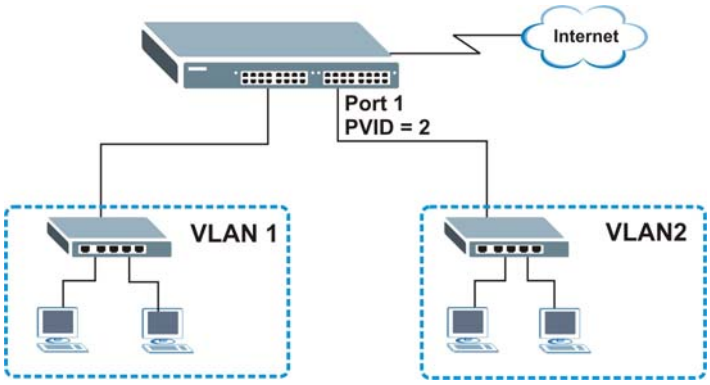
5 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

2.6 Setting Port VID

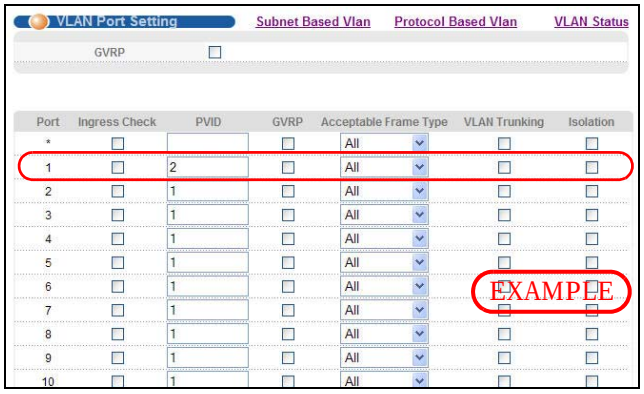
Use PVID to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

In the example network, configure 2 as the port VID on port 1 so that any untagged frames received on that port get sent to VLAN 2.

Figure 8 Initial Setup Network Example: Port VID



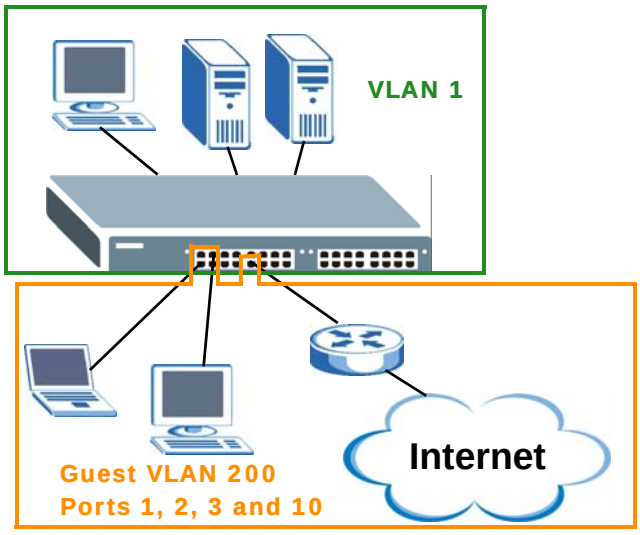
1 Click **Advanced Applications** and **VLAN** in the navigation panel. Then click the **VLAN Port Setting** link.



Enter 2 in the **PVID** field for port 1 and click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

2.7 How to Set Up a Guest VLAN

All ports on the Switch are in VLAN 1 by default. Say you enable IEEE 802.1x authentication on ports 1 to 8. Clients that connect to these ports should provide the correct user name and password in order to access the ports. You want to assign clients that connect to ports 1, 2 or 3 to a guest VLAN (200 for example) before they can authenticate with the authentication server. In this guest VLAN, clients can surf the Internet through the default gateway attached to port 10, but are not allowed to access other network resources, such as the mail server or local data base.

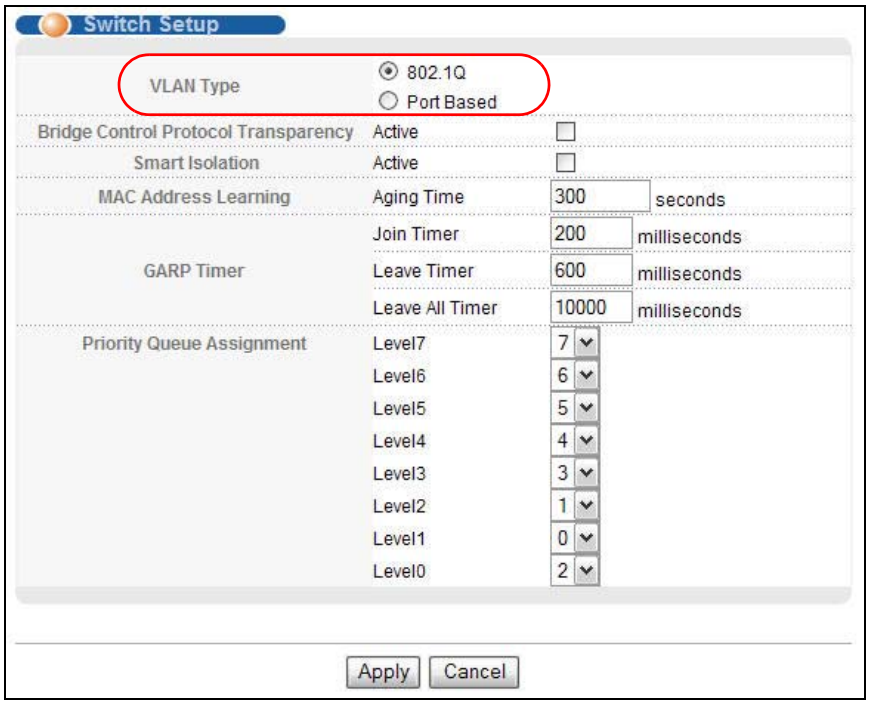


2.7.1 Creating a Guest VLAN

Follow the steps below to configure port 1, 2, 3 and 10 as a member of VLAN 200.

1 Access the web configurator through the Switch's management port.

2 Go to **Basic Setting > Switch Setup** and set the VLAN type to **802.1Q**. Click **Apply** to save the settings to the run-time memory.



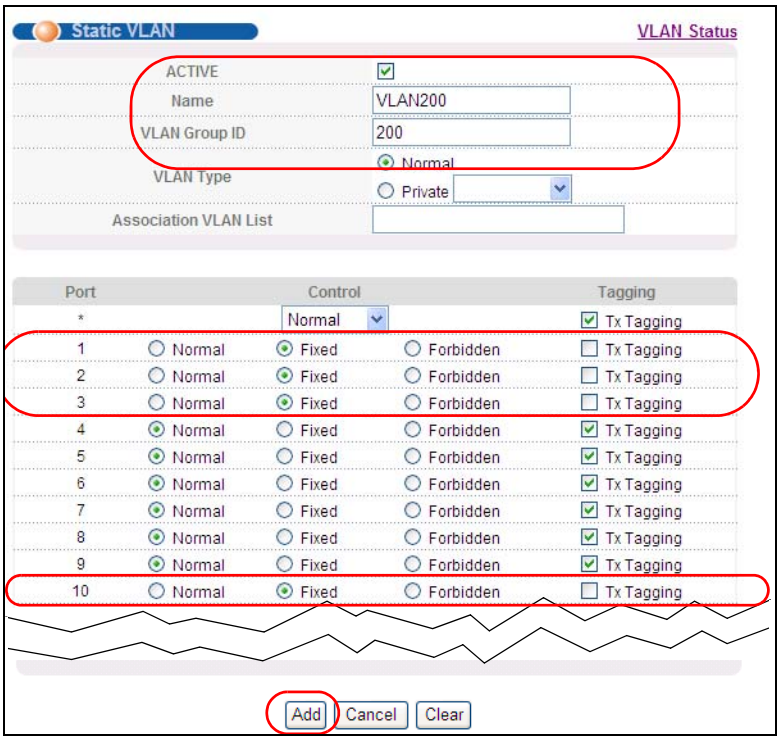
3 Click **Advanced Application > VLAN > Static VLAN**.

4 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name (VLAN 200 for example) in the **Name** field and enter 200 in the **VLAN Group ID** field.

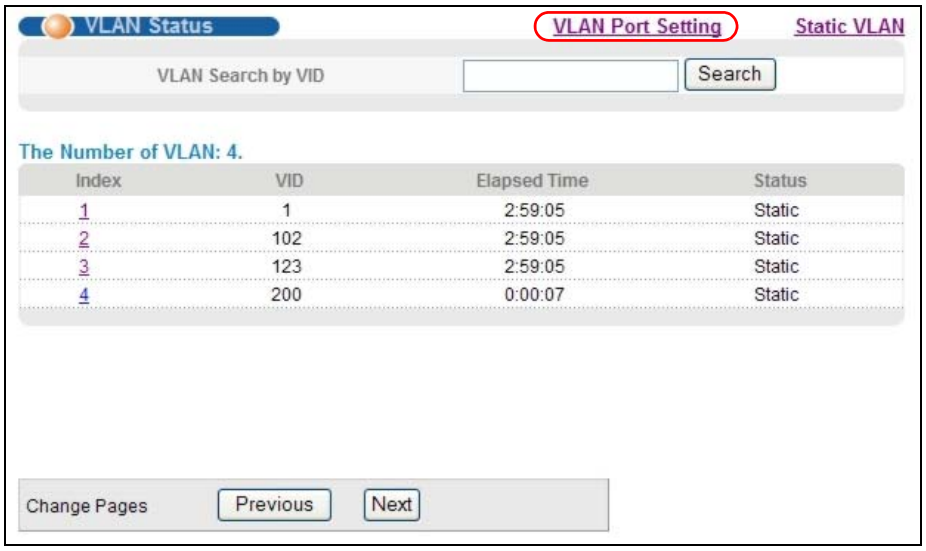
5 Select **Fixed** to configure ports 1, 2, 3 and 10 to be permanent members of this VLAN.

6 Clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending frames out of these ports.

7 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

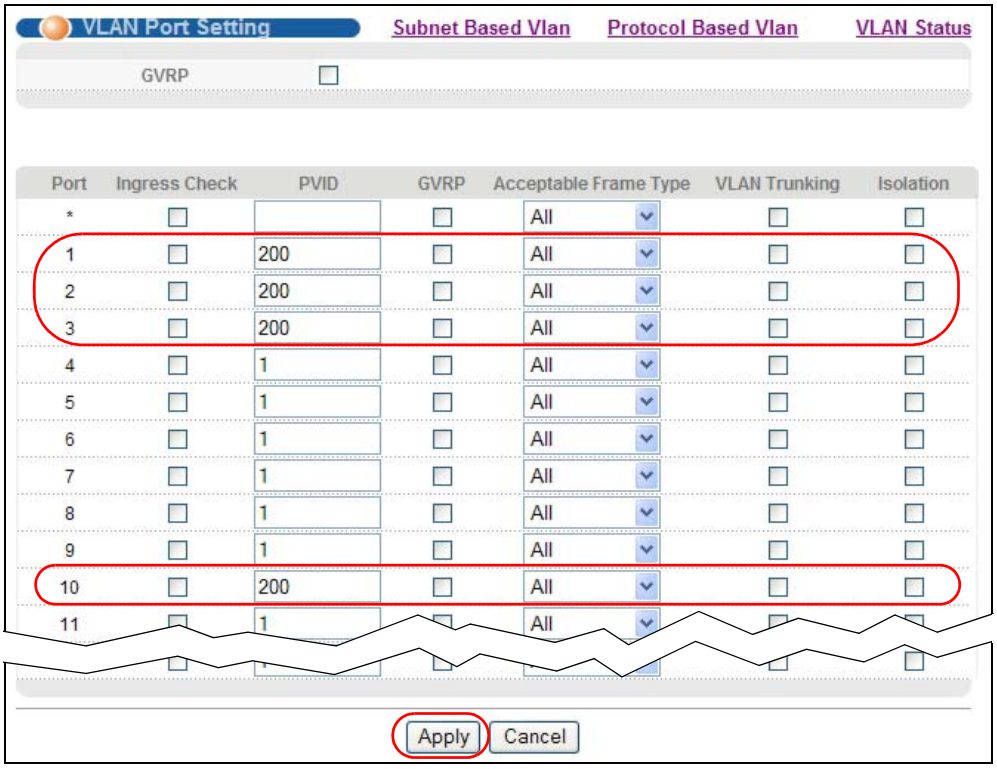


8 Click the **VLAN Status** link in the **Static VLAN** screen and then the **VLAN Port Setting** link in the **VLAN Status** screen.



9 Enter 200 in the **PVID** field for ports 1, 2, 3 and 10 to add a tag to incoming untagged frames received on these ports so that the frames are forwarded to the VLAN group that the tag defines.

10 Click **Apply** to save your changes back to the run-time memory.



11 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

2.7.2 Enabling IEEE 802.1x Port Authentication

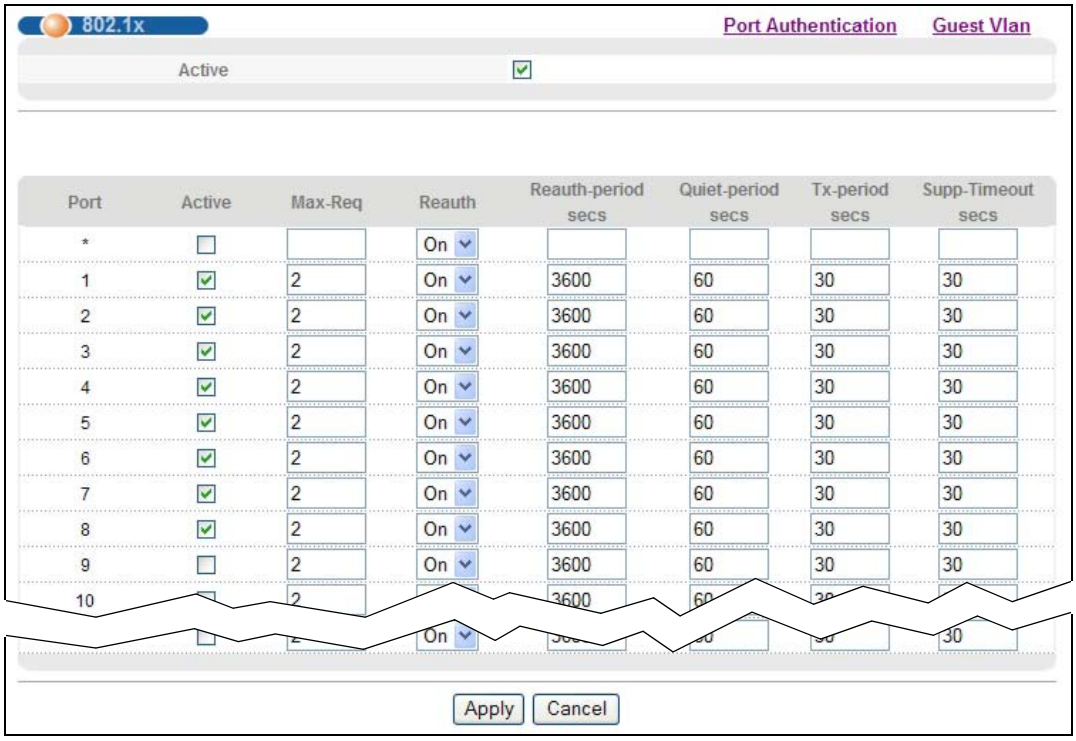
Follow the steps below to enable port authentication to validate access to ports 1~8 to clients based on a RADIUS server.

1 Click **Advanced Application** > **Port Authentication** and then the **Click Here** link for **802.1x**.

2 Select the first **Active** checkbox to enable 802.1x authentication on the Switch.

Select the **Active** checkboxes for ports 1 to 8 to turn on 802.1x authentication on the selected ports.

Click **Apply**.



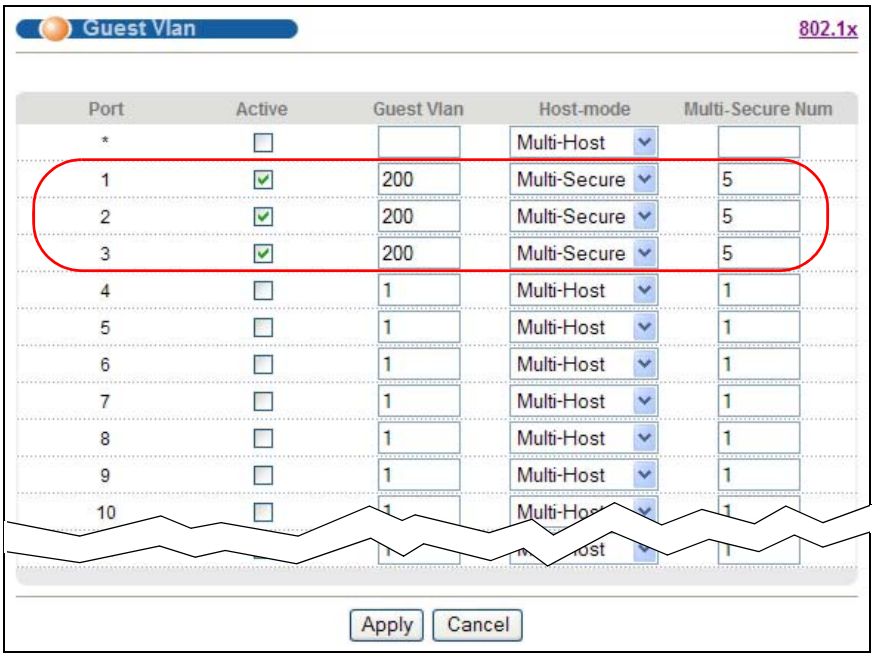
2.7.3 Enabling Guest VLAN

1 Click the **Guest Vlan** link in the **802.1x** screen.

2 Select **Active** and enter the guest VLAN ID (200 in this example) on ports 1, 2 and 3. The Switch puts unauthenticated clients in the specified guest VLAN.

Set **Host-mode** to **Multi-Secure** to have the Switch authenticate each client that connects to one of these ports, and specify the maximum number of clients that the Switch will authenticate on each of these port (5 in this example).

Click **Apply**.



3 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.

Clients that attach to port 1, 2 or 3 and fail to authenticate with the RADIUS server now should be in VLAN 200 and can access the Internet, but cannot communicate with devices in VLAN 1.

3

Switch Hardware Overview

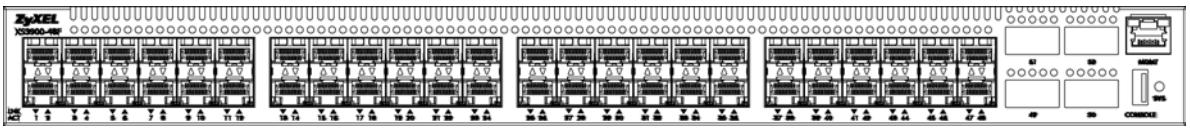
This chapter describes the front panel and rear panel of the Switch and shows you how to make the hardware connections.

- See the **Module Hardware Installation Guide** to see how to install the power and fan modules in the Switch.
- See the **Rack Mounting Hardware Installation Guide** to see how to use the rack mounting kit to install the Switch in a rack.

3.1 Front Panel Connections

The figure below shows the front panel of the Switch.

Figure 9 Front Panel



The following table describes the ports.

Table 7 Panel Connections

CONNECTOR	DESCRIPTION
48 10GbE SFP+ Ports	Use Small Form-Factor Pluggable Plus (SFP+) transceivers in these ports for fiber-optic or copper connections to a server, Ethernet switch or router. You can also insert an SFP+ Direct Attach Copper (DAC) in the SFP+ slot.
Four 40GbE QSFP+ Ports	Use Quad Small Form-Factor Pluggable Plus (QSFP+) transceivers in these ports for fiber-optic or copper connections to a server, Ethernet switch or router.
Console Port	Connect this port to your computer (using a USB cable) if you want to configure the Switch using the command line interface (CLI) via the console port. You don't need to install a USB driver to use this port.
RJ-45 out-of-band management port	Connect an Ethernet cable to this port for dedicated management of the Switch. You can configure the Switch via Telnet or the web configurator. The default IP address of the management port is 192.168.0.1 with a subnet mask of 255.255.255.0. This port can operate at 10/100/1000 Mbps speeds and is not VLAN-aware.

3.1.1 (Q)SFP+ Transceiver Slots

These are 48 slots for Small Form-Factor Pluggable Plus (SFP+) transceivers and four for Quad Small Form-Factor Pluggable Plus (QSFP+) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. Use a transceiver to connect a fiber-optic cable to the Switch. The Switch does not come with transceivers. You must use transceivers that comply with the Small

Form-Factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

You can change transceivers while the Switch is operating. You can use different transceivers to connect to Ethernet switches with different types of fiber-optic connectors.

- Type: SFP+ or QSFP+ connection interface
- Connection speed: 1, 10 or 40 Gigabit per second (Gbps)

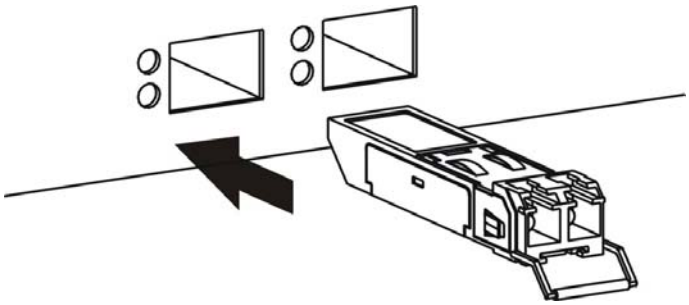
To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

3.1.1.1 Transceiver Installation

Use the following steps to install a (Q)SFP+ transceiver (the graphics are indicative only).

1 Insert the transceiver into the slot with the exposed section of PCB board facing down.

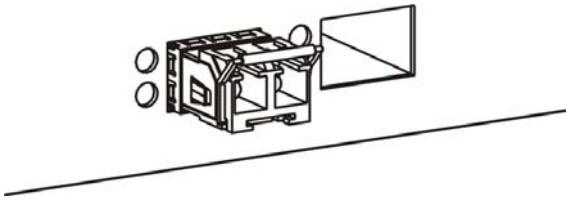
Figure 10 Transceiver Installation Example



2 Press the transceiver firmly until it clicks into place.

3 The Switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.

Figure 11 Installed Transceiver

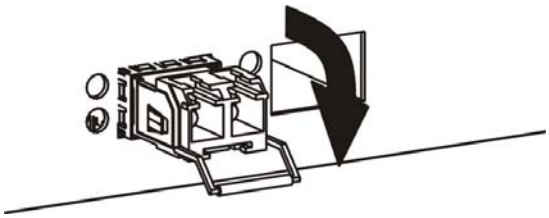


3.1.1.2 Transceiver Removal

Use the following steps to remove a (Q)SFP+ transceiver.

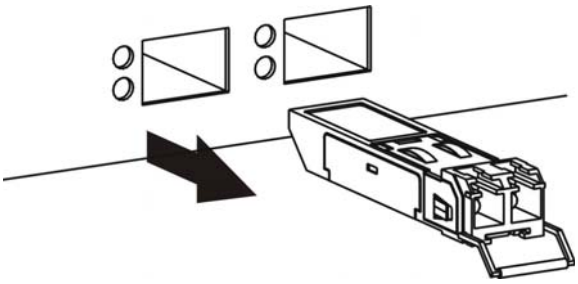
1 Open the transceiver's latch (latch styles vary).

Figure 12 Opening the Transceiver's Latch Example



2 Pull the transceiver out of the slot.

Figure 13 Transceiver Removal Example

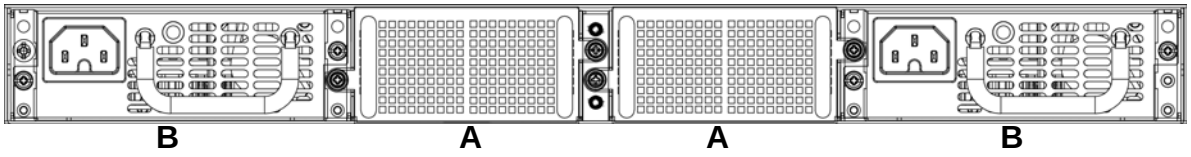


3.2 Rear Panel

The following figures show the rear panel of the Switch. The rear panels contain:

- Two slots for fan modules (**A**)
- Two slots for power modules with power receptacles (**B**)

Figure 14 Rear Panel



3.2.1 Power Connection

Make sure you are using the correct power source and that no objects obstruct the airflow of the fans in both fan and power modules.

The Switch uses two power supply modules, one of which is redundant, so if one power module fails the system can operate on the remaining module. The power connections are on the front of each power module.

Use the following procedure to connect the Switch to a power source after you have installed it in a rack.

1 Connect the female end of the power cord to the module power socket.

2 Connect the other end of the cord to a power outlet.

The power modules can be disconnected from the power source individually. Use the following procedure to disconnect the Switch from a power source.

1 Disconnect the power cord from the power outlet.

2 Disconnect the power cord from the module power socket.

3.3 Switch LEDs

The following table describes the Switch LEDs.

Table 8 Switch LEDs

LED	COLOR	STATUS	DESCRIPTION
SYS	Green	Blinking	The Switch is rebooting and performing self-diagnostic tests.
		On	The Switch is on and functioning properly.
	Amber	On	The Switch is overheating due to abnormal voltage or fan speed.
		Off	The power is off or the Switch is not ready or malfunctioning.
MGMT			
LINK	Green	On	The **MGMT** port is connected at 1000 Mbps.
	Amber	On	The **MGMT** port is connected at 10 or 100 Mbps.
		Off	The **MGMT** port is not up or not connected to an Ethernet device.
ACTIVITY	Green	Blinking	The Switch is transmitting or receiving to/from an Ethernet device through the **MGMT** port.
		Off	The Switch is not transmitting or receiving to/from an Ethernet device through the **MGMT** port.
1-48	Green	Blinking	The port is receiving or transmitting data at 1 or 10 Gbps.
		On	The port has a successful 1 or 10 Gbps connection.
		Off	This link is disconnected.
49-52	Green	Blinking	The port is receiving or transmitting data at 40 Gbps.
		On	The port has a successful 40 Gbps connection.
		Off	This link is disconnected.

4

The Web Configurator

This section introduces the configuration and functions of the web configurator.

4.1 Introduction

The web configurator is an HTML-based management interface that allows easy Switch setup and management via Internet browser. Use Internet Explorer 6.0 and later or Firefox 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

4.2 System Login

1. Start your web browser.
2. Type “http://” and the IP address of the Switch (for example, the default management IP address is 192.168.1.1 through an in-band (non-**MGMT**) port and 192.168.0.1 through the **MGMT** port) in the Location or Address field. Press [ENTER].

3 The login screen appears. The default username is **admin** and associated default password is **1234**. The date and time display as shown if you have not configured a time server nor manually entered a time and date in the **General Setup** screen.

Figure 15 Web Configurator: Login

Connect to 192.168.0.1
The server 192.168.0.1 at XGS4700 at Thu Jan 1 00:04:31 1970 requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

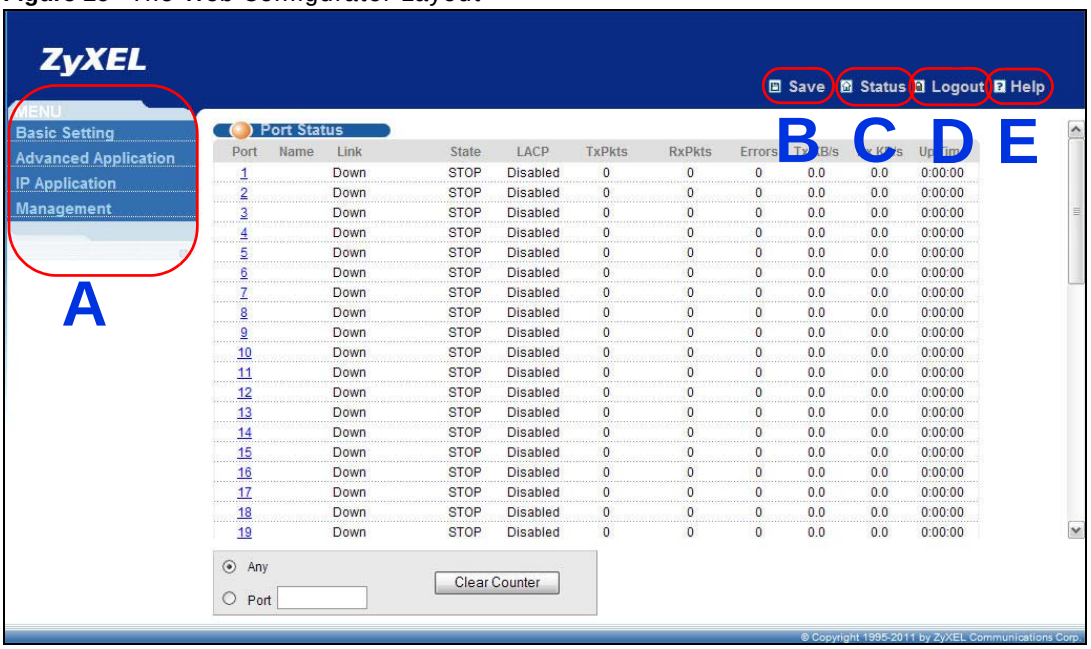
4 Click **OK** to view the first web configurator screen.

4.3 The Web Configurator Layout

The **Status** screen is the first screen that displays when you access the web configurator.

The following figure shows the navigating components of a web configurator screen.

Figure 16 The Web Configurator Layout



A - Click the menu items to open submenu links, and then click on a submenu link to open the screen in the main window.

B, **C**, **D**, **E** - These are quick links which allow you to perform certain tasks no matter which screen you are currently working in.

B - Click this link to save your configuration into the Switch's nonvolatile memory. Nonvolatile memory is saved in the configuration file from which the Switch booted from and it stays the same even if the Switch's power is turned off. See Section 35.3 on page 270 for information on saving your settings to a specific configuration file.

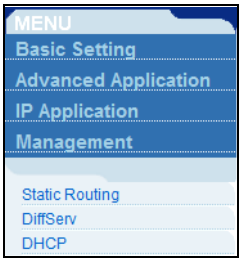
C - Click this link to go to the status page of the Switch.

D - Click this link to log out of the web configurator.

E - Click this link to display web help pages. The help pages provide descriptions for all of the configuration screens.

In the navigation panel, click a main link to reveal a list of submenu links.

Table 9 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
			

The following table describes the links in the navigation panel.

Table 10 Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system and hardware monitoring information.
General Setup	This link takes you to a screen where you can configure general identification information and time settings for the Switch.
Switch Setup	This link takes you to a screen where you can set up global Switch parameters such as VLAN type, MAC address learning, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address, subnet mask (necessary for Switch management) and DNS (domain name server) and set up to 64 IP routing domains.
Port Setup	This link takes you to screens where you can configure speed, flow control and priority settings for individual Switch ports.
Advanced Application	
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the Switch Setup menu). You can also configure a protocol based VLAN or a subnet based VLAN in these screens.
Static MAC Forwarding	This link takes you to screens where you can configure static MAC addresses for a port. These static MAC addresses do not age out.

Table 10 Navigation Panel Links (continued)

LINK	DESCRIPTION
Static Multicast Forwarding	This link takes you to a screen where you can configure static multicast MAC addresses for port(s). These static multicast MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the RSTP/MRSTP/MSTP to prevent network loops.
Bandwidth Control	This link takes you to screens where you can cap the maximum bandwidth allowed on a port.
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference.
Link Aggregation	This link takes you to screen where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure IEEE 802.1x port authentication as well as MAC authentication for clients communicating via the Switch.
Port Security	This link takes you to a screen where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
Classifier	This link takes you to a screen where you can configure the Switch to group packets based on the specified criteria.
Policy Rule	This link takes you to a screen where you can configure the Switch to perform special treatment on the grouped packets.
Queuing Method	This link takes you to a screen where you can configure queuing with associated queue weights for each port.
VLAN Stacking	This link takes you to screens where you can activate and configure VLAN stacking.
Multicast	This link takes you to screen where you can configure various multicast features, IGMP snooping and create multicast VLANs.
AAA	This link takes you to a screen where you can configure authentication, authorization and accounting services via external servers. The external servers can be either RADIUS (Remote Authentication Dial-In User Service) or TACACS+ (Terminal Access Controller Access-Control System Plus).
IP Source Guard	This link takes you to screens where you can configure filtering of unauthorized DHCP and ARP packets in your network.
Loop Guard	This link takes you to a screen where you can configure protection against network loops that occur on the edge of your network.
VLAN Mapping	This link takes you to screens where you can configure VLAN mapping settings on the Switch.
Layer 2 Protocol Tunneling	This link takes you to a screen where you can configure L2PT (Layer 2 Protocol Tunneling) settings on the Switch.
sFlow	This link takes you to screens where you can configure sFlow settings on the Switch.
PPPoE	This link takes you to screens where you can configure how the Switch gives a PPPoE termination server additional subscriber information that the server can use to identify and authenticate a PPPoE client.
Errdisable	This link takes you to a screen where you can configure CPU protection and error disable recovery.
Private VLAN	This link takes you to screens where you can configure private VLAN port mapping.
IP Application	
Static Route	This link takes you to a screen where you can configure static routes. A static route defines how the Switch should forward traffic by configuring the TCP/IP parameters manually.

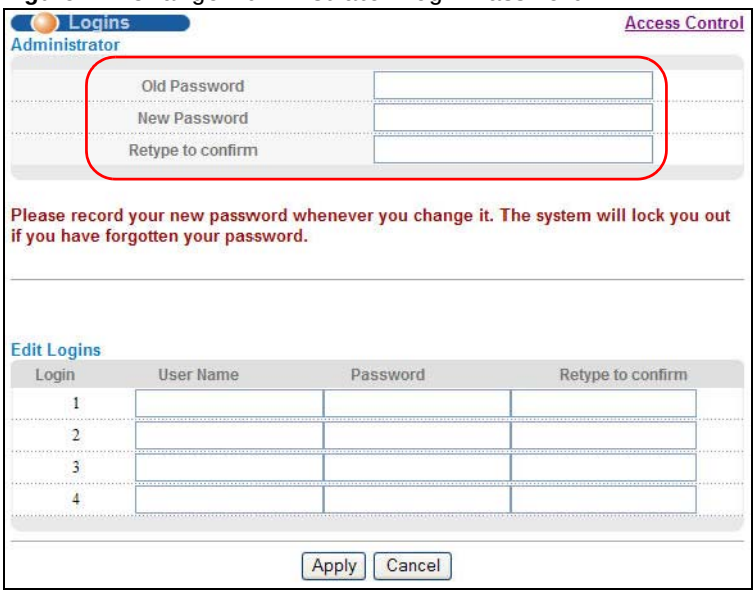
Table 10 Navigation Panel Links (continued)

LINK	DESCRIPTION
DiffServ	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
DHCP	This link takes you to screens where you can configure the DHCP settings.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Diagnostic	This link takes you to screens where you can view system logs and can test port(s).
Syslog	This link takes you to screens where you can setup system logs and a system log server.
Cluster Management	This link takes you to a screen where you can configure clustering management and view its status.
MAC Table	This link takes you to a screen where you can view the MAC address and VLAN ID of a device attach to a port. You can also view what kind of MAC address it is.
ARP Table	This link takes you to a screen where you can view the MAC address – IP address resolution table.
Configure Clone	This link takes you to a screen where you can copy attributes of one port to (an)other port(s).

4.3.1 Change Your Password

After you log in for the first time, it is recommended you change the default administrator password. Click **Management** > **Access Control > Logins** to display the next screen.

Figure 17 Change Administrator Login Password



4.4 Saving Your Configuration

When you are done modifying the settings in a screen, click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

Click the **Save** link in the upper right hand corner of the web configurator to save your configuration to nonvolatile memory. Nonvolatile memory refers to the Switch's storage that remains even if the Switch's power is turned off.

Note: Use the **Save** link when you are done with a configuration session.

4.5 Switch Lockout

You could block yourself (and all others) from using in-band-management (managing through the data ports) if you do one of the following:

1. Delete the management VLAN (default is VLAN 1).
2. Delete all port-based VLANs with the CPU port as a member. The "CPU port" is the management port of the Switch.
3. Filter all traffic to the CPU port.
4. Disable all ports.
5. Misconfigure the text configuration file.
6. Forget the password and/or IP address.
7. Prevent all services from accessing the Switch.
8. Change a service port number but forget it.

Note: Be careful not to lock yourself and others out of the Switch. If you do lock yourself out, try using out-of-band management (via the management port) to configure the Switch.

4.6 Resetting the Switch

If you lock yourself (and others) from the Switch or forget the administrator password, you will need to reload the factory-default configuration file or reset the Switch back to the factory defaults.

4.6.1 Reload the Configuration File

Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop

bit and flow control set to none. The password will also be reset to “1234” and the IP address to 192.168.1.1.

To upload the configuration file, do the following:

1. Connect to the console port using a computer with terminal emulation software. See Section 3.2 on page 51 for details.
2. Disconnect and reconnect the Switch’s power to begin a session. When you reconnect the Switch’s power, you will see the initial screen.
3. When you see the message “Press any key to enter Debug Mode within 3 seconds ...” press any key to enter debug mode.
4. Type atlc after the “Enter Debug Mode” message.
5. Wait for the “Starting XMODEM upload” message before activating XMODEM upload on your terminal.
6. After a configuration file upload, type atgo to restart the Switch.

Figure 18 Resetting the Switch: Via the Console Port

```
Bootbase Version: V1.00 | 01/13/2011 19:34:13
RAM: Size = 524288 Kbytes

ZyNOS Version: V4.00(BVG.0)b6 | 01/28/2011 14:44:24

Press any key to enter debug mode within 3 seconds.
.................................
Enter Debug Mode
ras> atlc
Starting XMODEM upload (CRC mode)....
CCCCCCCCCCCCCCC
Total  393216 bytes received.
Erasing..
.............................................................
OK
ras> atgo
```

The Switch is now reinitialized with a default configuration file including the default password of “1234”.

4.7 Logging Out of the Web Configurator

Click **Logout** in a screen to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session for security reasons.

Figure 19 Web Configurator: Logout Screen

4.8 Help

The web configurator's online help has descriptions of individual screens and some supplementary information.

Click the **Help** link from a web configurator screen to view an online help description of that screen.

PART II
Technical Reference

5

System Status and Port Statistics

This chapter describes the system status (web configurator home page) and port details screens.

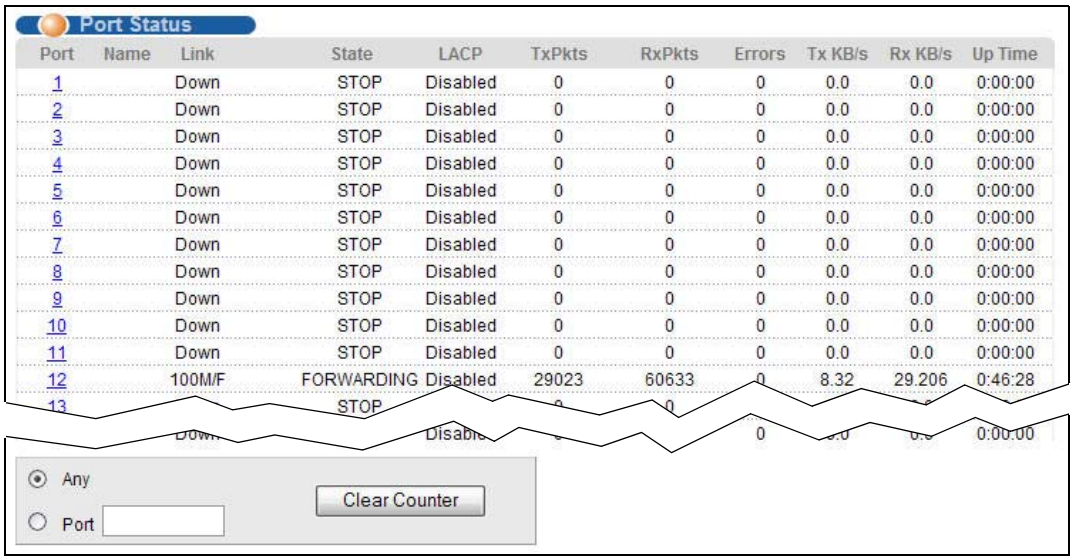
5.1 Overview

The home screen of the web configurator displays a port statistical summary with links to each port showing statistical details.

5.2 Port Status Summary

To view the port statistics, click **Status** in all web configurator screens to display the **Status** screen as shown next.

Figure 20 Port Status


Port Status
Port Name Link State LACP TxPkts RxPkts Errors Tx KB/s Rx KB/s Up Time
1 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
2 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
3 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
4 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
5 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
6 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
7 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
8 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
9 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
10 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
11 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
12 100M/F FORWARDING Disabled 29023 60633 0 8.32 29.206 0:46:28
13 STOP
0 0:00:00
Any
Port
Clear Counter

The following table describes the labels in this screen.

Table 11 Port Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port. Click a port number to display the **Port Details** screen (refer to Figure 21 on page 67).
Name	This is the name you assigned to this port in the **Basic Setting** > **Port Setup** screen.

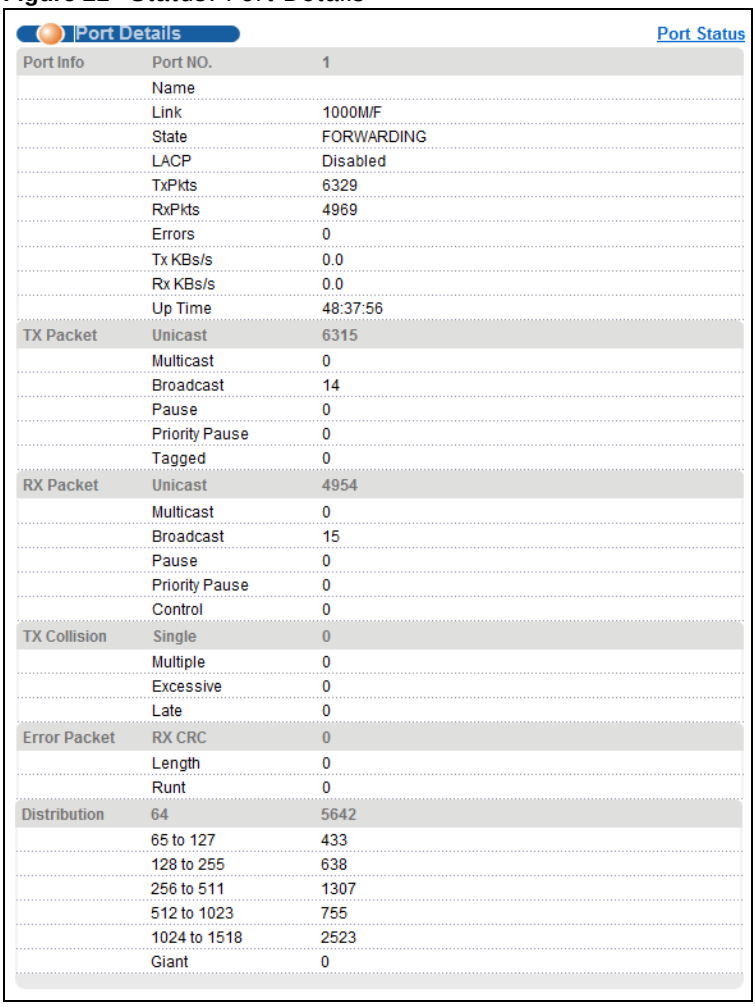
Table 11 Port Status (continued)

LABEL	DESCRIPTION
Link	This field displays the speed (**1000M** for 1000 Mbps, **10G** for 10 Gbps, and **40G** for 40 Gbps) and the duplex (**F** for full duplex). This field displays **Down** if the port is not connected to any device.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. (See Section 11.1.3 on page 108 for more information). If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**.
LACP	This fields displays whether LACP (Link Aggregation Control Protocol) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the transmission speed of data sent on this port in kilobytes per second.
Rx KB/s	This field shows the transmission speed of data received on this port in kilobytes per second.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Clear Counter	Type a port number, select **Port** and then click **Clear Counter** to erase the recorded statistical information for that port, or select **Any** to clear statistics for all ports.

5.2.1 Status: Port Details

Click a number in the **Port** column in the **Status** screen to display individual port statistics. Use this screen to check status and detailed performance data about an individual port on the Switch.

Figure 21 Status: Port Details



Port Info	Port NO.	1
	Name	
	Link	1000M/F
	State	FORWARDING
	LACP	Disabled
	TxPkts	6329
	RxPkts	4969
	Errors	0
	Tx KBs/s	0.0
	Rx KBs/s	0.0
	Up Time	48:37:56
TX Packet	Unicast	6315
	Multicast	0
	Broadcast	14
	Pause	0
	Priority Pause	0
	Tagged	0
RX Packet	Unicast	4954
	Multicast	0
	Broadcast	15
	Pause	0
	Priority Pause	0
	Control	0
TX Collision	Single	0
	Multiple	0
	Excessive	0
	Late	0
Error Packet	RX CRC	0
	Length	0
	Runt	0
Distribution	64	5642
	65 to 127	433
	128 to 255	638
	256 to 511	1307
	512 to 1023	755
	1024 to 1518	2523
	Giant	0

The following table describes the labels in this screen.

Table 12 Status > Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing.
Name	This field displays the name of the port.
Link	This field displays the speed (**1000M** for 1000 Mbps, **10G** for 10 Gbps, and **40G** for 40 Gbps) and the duplex (**F** for full duplex).
Status	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 11.1.3 on page 108 for more information). If STP is disabled, this field displays **FORWARDING** if the link is up, otherwise, it displays **STOP**.
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port
RxPkts	This field shows the number of received frames on this port
Errors	This field shows the number of received errors on this port.
Tx KB/s	This field shows the transmission speed of data sent on this port in kilobytes per second.

Table 12 Status > Port Details (continued)

LABEL	DESCRIPTION
Rx KB/s	This field shows the transmission speed of data received on this port in kilobytes per second.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet The following fields display detailed information about frames transmitted.	
Unicast	This field shows the number of good unicast frames transmitted.
Multicast	This field shows the number of good multicast frames transmitted.
Broadcast	This field shows the number of good broadcast frames transmitted.
Pause	Pause is a flow control mechanism that notifies the sender to slow transmission if the receiver's buffers are (almost) full. This field shows the number of 802.3x Pause frames transmitted.
Priority Pause	You may use commands to request which Pause frames are stopped according to priority (0 to 7). For example, you may request the sender to stop Pause frames with priority equal to 3 and 4. This field shows the number of 802.1Qbb Pause frames transmitted.
Tagged	This field shows the number of frames with VLAN tags transmitted.
Rx Packet The following fields display detailed information about frames received.	
Unicast	This field shows the number of good unicast frames received.
Multicast	This field shows the number of good multicast frames received.
Broadcast	This field shows the number of good broadcast frames received.
Pause	Pause is a flow control mechanism that notifies the sender to slow transmission if the receiver's buffers are (almost) full. This field shows the number of 802.3x Pause frames received.
Priority Pause	This field shows the number of 802.1Qbb Pause frames received.
Control	This field shows the number of control frames received (including those with CRC error) but it does not include the 802.3x Pause frames.
TX Collision The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted frames for which transmission was inhibited by more than one collision.
Excessive	This is a count of frames for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the frames have already been transmitted.
Error Packet	The following fields display detailed information about frames received that were in error.
RX CRC	This field shows the number of frames received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of frames received with a length that was out of range.
Runt	This field shows the number of frames received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	

Table 12 Status > Port Details (continued)

LABEL	DESCRIPTION
64	This field shows the number of frames (including bad frames) received that were 64 octets in length.
65-127	This field shows the number of frames (including bad frames) received that were between 65 and 127 octets in length.
128-255	This field shows the number of frames (including bad frames) received that were between 128 and 255 octets in length.
256-511	This field shows the number of frames (including bad frames) received that were between 256 and 511 octets in length.
512-1023	This field shows the number of frames (including bad frames) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of frames (including bad frames) received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of frames (including bad frames) received that were between 1519 octets and the maximum frame size. The maximum frame size varies depending on your switch model.

6

Basic Setting

This chapter describes how to configure the **System Info, General Setup**, **Switch Setup**, **IP Setup** and **Port Setup** screens.

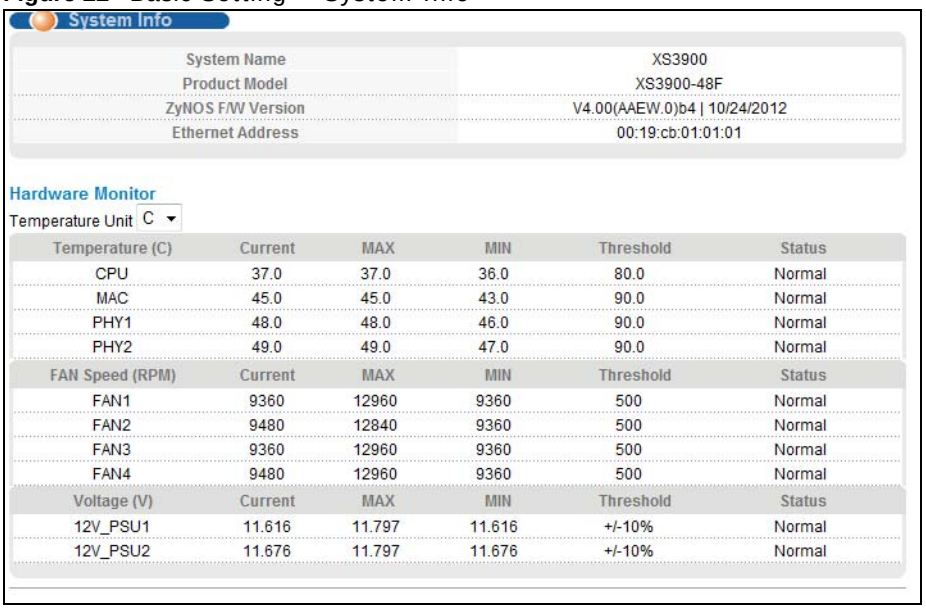
6.1 Overview

The **System Info** screen displays general Switch information (such as firmware version number) and hardware polling information (such as fan speeds). The **General Setup** screen allows you to configure general Switch identification information. The **General Setup** screen also allows you to set the system time manually or get the current time and date from an external server when you turn on your Switch. The real time is then displayed in the Switch logs. The **Switch Setup** screen allows you to set up and configure global Switch features. The **IP Setup** screen allows you to configure Switch outband and inband IP addresses, subnet mask(s) and DNS (domain name server) for management purposes. The **Port Setup** screen allows you to enable or disable a port on the Switch and configure the port settings, such as the speed and duplex mode.

6.2 System Information

In the navigation panel, click **Basic Setting** > **System Info** to display the screen as shown. You can check the firmware version number and monitor the Switch temperature, fan speeds and voltage in this screen.

Figure 22 Basic Setting > System Info


System Info
System Name XS3900
Product Model XS3900-48F
ZyNOS F/W Version V4.00(AAEW.0)b4 | 10/24/2012
Ethernet Address 00:19:cb:01:01:01
Hardware Monitor
Temperature Unit C
Temperature (C) Current MAX MIN Threshold Status
CPU 37.0 37.0 36.0 80.0 Normal
MAC 45.0 45.0 43.0 90.0 Normal
PHY1 48.0 48.0 46.0 90.0 Normal
PHY2 49.0 49.0 47.0 90.0 Normal
FAN Speed (RPM) Current MAX MIN Threshold Status
FAN1 9360 12960 9360 500 Normal
FAN2 9480 12840 9360 500 Normal
FAN3 9360 12960 9360 500 Normal
FAN4 9480 12960 9360 500 Normal
Voltage (V) Current MAX MIN Threshold Status
12V_PSU1 11.616 11.797 11.616 +/-10% Normal
12V_PSU2 11.676 11.797 11.676 +/-10% Normal

The following table describes the labels in this screen.

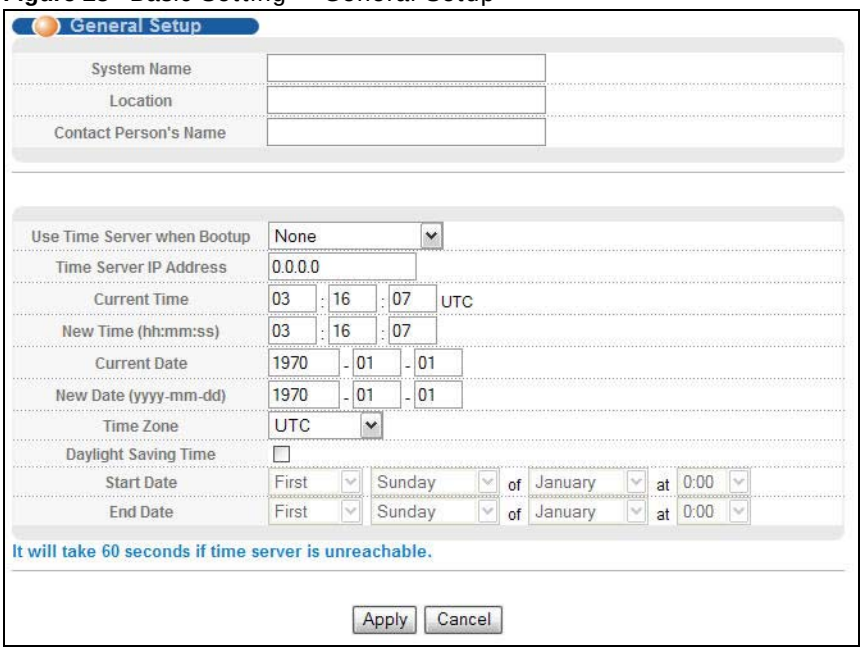
Table 13 Basic Setting > System Info

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the Switch for identification purposes.
Product Model	This field displays the model number of the Switch.
ZyNOS F/W Version	This field displays the version number of the Switch 's current firmware including the date created.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the Switch.
Hardware Monitor	
Temperature Unit	The Switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	**CPU**, **PHY**, and **MAC** refer to the location of the temperature sensors on the Switch printed circuit board.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays **Normal** for temperatures below the threshold and **Error** for those above.
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in RPM.
MIN	This field displays this fan's minimum speed measured in RPM. “<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	**Normal** indicates that this fan is functioning above the minimum speed. **Error** indicates that this fan is functioning below the minimum speed.
Voltage (V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the percentage tolerance of the voltage with which the Switch still works.
Status	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Error** is displayed.

6.3 General Setup

Use this screen to configure general settings such as the system name and time. Click **Basic Setting** and **General Setup** in the navigation panel to display the screen as shown.

Figure 23 Basic Setting > General Setup



The following table describes the labels in this screen.

Table 14 Basic Setting > General Setup

LABEL	DESCRIPTION
System Name	Type a descriptive name for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Location	Type the geographic location of your Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Contact Person's Name	Type the name of the person in charge of this Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Use Time Server when Bootup	Type the time service protocol that your timeserver uses. Not all time servers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. When you select the **Daytime (RFC 867)** format, the Switch displays the day, month, year and time with no time zone adjustment. When you use this format, it is recommended that you use a Daytime timeserver within your geographical time zone. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to Time (RFC-868). **None** is the default value. Enter the time manually. Each time you turn on the Switch, the time and date will be reset to 1970-1-1 0:0.
Time Server IP Address	Type the IP address of your timeserver. The Switch searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.

Table 14 Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the **Current Time** field after you click **Apply**.
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the **Current Date** field after you click **Apply**.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Daylight Saving Time	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Saving Time**. The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and **2:00**. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Saving Time**. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and **2:00**. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October** and the last field depends on your time zone. In Germany for instance, you would select **2:00** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.4 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user on the same network.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast frames go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

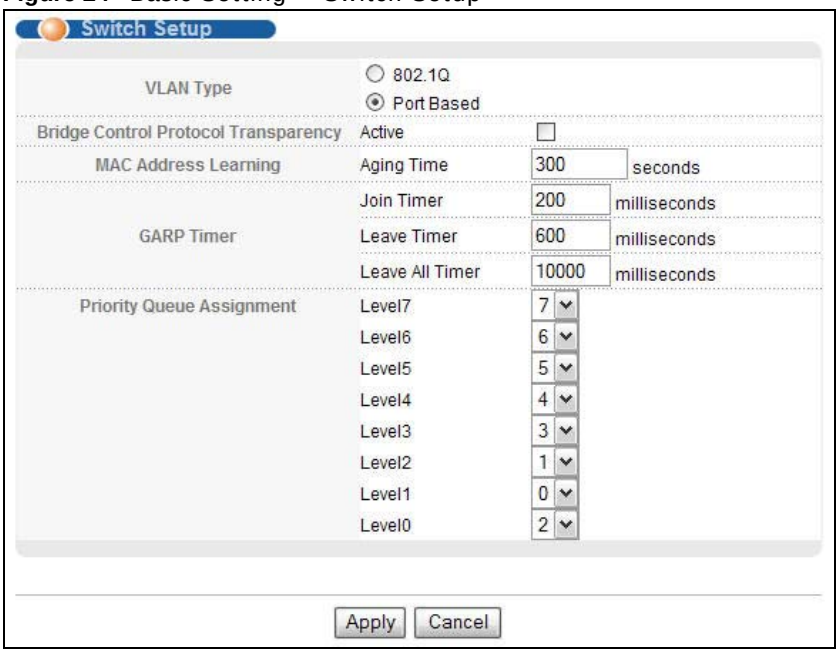
Note: VLAN is unidirectional; it only governs outgoing traffic.

See Chapter 7 on page 81 for information on port-based and 802.1Q tagged VLANs.

6.5 Switch Setup Screen

Click **Basic Setting** and then **Switch Setup** in the navigation panel to display the screen as shown. The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen. Refer to the chapter on VLAN.

Figure 24 Basic Setting > Switch Setup



The following table describes the labels in this screen.

Table 15 Basic Setting > Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose **802.1Q** or **Port Based**. The **VLAN Setup** screen changes depending on whether you choose **802.1Q** VLAN type or **Port Based** VLAN type in this screen. See Chapter 7 on page 81 for more information.
Bridge Control Protocol Transparency	Select **Active** to allow the Switch to handle bridging control protocols (STP, for example). You also need to define how to treat a BPDU in the **Port Setup** screen.
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.
Aging Time	Enter a time from 10 to 1000000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).

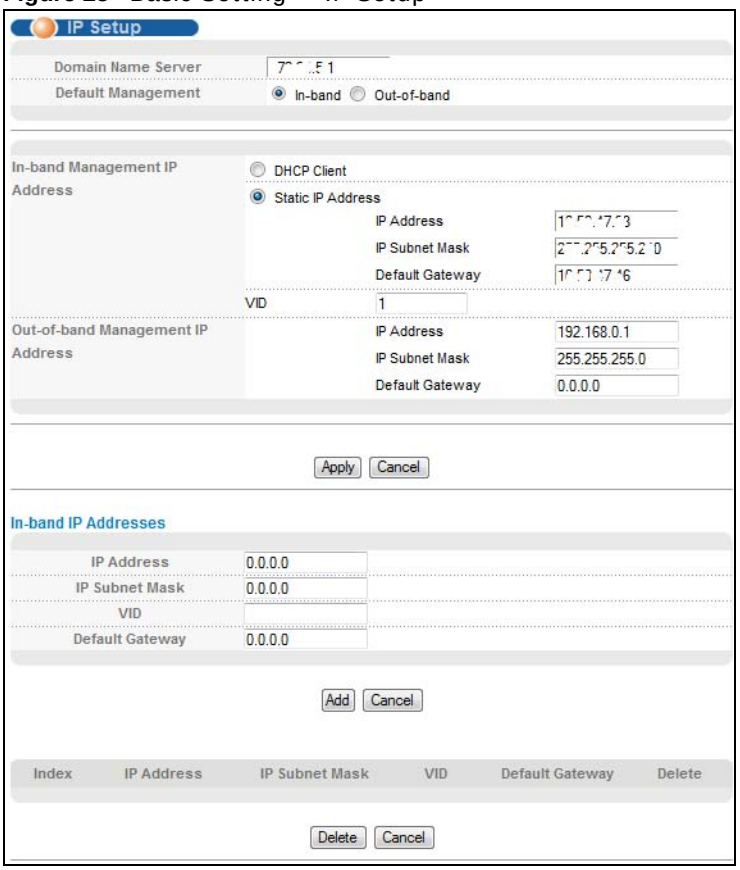
Table 15 Basic Setting > Switch Setup (continued)

LABEL	DESCRIPTION
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a **Join** message using GARP. Declarations are withdrawn by issuing a **Leave** message. A **Leave All** message terminates all registrations. GARP timers set declaration timeout values. See Chapter 7 on page 81 for more background information.	
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a **Join Period** timer. The allowed **Join Time** range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See Chapter 7 on page 81 for more background information.
Leave Timer	Leave Time sets the duration of the **Leave Period** timer for GVRP in milliseconds. Each port has a single **Leave Period** timer. Leave Time must be two times larger than **Join Timer**; the default is 600 milliseconds.
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer.
Priority Queue Assignment IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the following fields to configure the priority level-to-physical queue mapping. The Switch has eight physical queues that you can map to the 8 priority levels. On the Switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.	
Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).	
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.6 IP Setup

Use the **IP Setup** screen to configure the default gateway device, the default domain name server and add IP domains.

Figure 25 Basic Setting > IP Setup



The following table describes the labels in this screen.

Table 16 Basic Setting > IP Setup

LABEL	DESCRIPTION
Domain Name Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
Default Management	Specify which traffic flow (**In-Band** or **Out-of-band**) the Switch is to send frames originating from itself (such as SNMP traps) or frames with unknown source. Select **Out-of-band** to have the Switch send the frames to the management port labelled **MGMT**. This means that device(s) connected to the other port(s) do not receive these frames. Select **In-Band** to have the Switch send the frames to all ports except the management port (labelled **MGMT**) to which connected device(s) do not receive these frames.
In-band Management IP Address - Use these fields to set the settings for the in-band management port.	
DHCP Client	Select this to have the in-band management port receive an IP address from an external DHCP server.
Static IP Address	Select this to give the in-band management port a fixed IP address, subnet mask and default gateway.

Table 16 Basic Setting > IP Setup (continued)

LABEL	DESCRIPTION
IP Address	Enter the in-band management port IP address of your Switch in dotted decimal notation. For example, 192.168.1.1.
IP Subnet Mask	Enter the in-band management port IP subnet mask of your Switch in dotted decimal notation, for example, 255.255.255.0.
Default Gateway	Enter the in-band management port IP address of the default outgoing gateway in dotted decimal notation, for example, 192.168.1.254
VID	Enter the VLAN identification number to which the in-band management port belongs.
Out-of-band Management IP Address - use these fields to set the settings for the out-of-band management port.	
IP Address	Enter the out-of-band management IP address of your Switch in dotted decimal notation. For example, 192.168.0.1.
IP Subnet Mask	Enter the IP subnet mask of your Switch in dotted decimal notation, for example, 255.255.255.0.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example, 192.168.0.254
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
In band IP address	You can create up to 64 IP addresses, which are used to access and manage the Switch from the ports belonging to the pre-defined VLAN(s). You must configure a VLAN first.
IP Address	Enter the IP address for managing the Switch by the members of the VLAN specified in the VID field below.
IP Subnet Mask	Enter the IP subnet mask in dotted decimal notation.
VID	Type the VLAN group identification number.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation.
Add	Click Add to insert the entry to the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Index	This field displays the index number of an entry.
IP Address	This field displays IP address of the Switch in the IP domain.
IP Subnet Mask	This field displays the subnet mask of the Switch in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the Switch.
Default Gateway	This field displays the the IP address of the default outgoing gateway.
Delete	Click **Delete** to remove the selected entry from the summary table. Note: Deleting all IP subnets locks you out of the Switch.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

6.7 Port Setup

Use this screen to configure Switch port settings.

6.7.1 Auto-negotiation

Auto-negotiation allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.

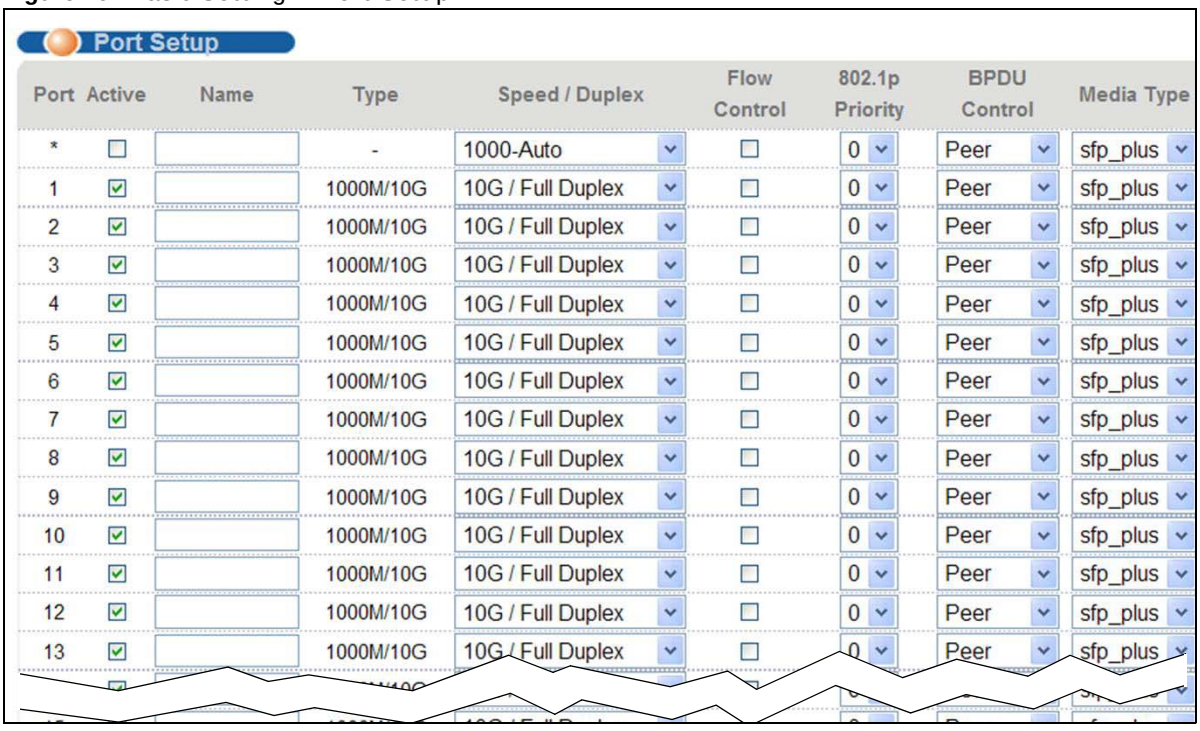
Both 1000-Auto and 1000M/Full Duplex operate at 1Gbps speed, in full-duplex mode. The differences are as follows:

Table 17 1000-Auto Vs 1000M/Full Duplex

SWITCH	PEER	RESULT
1000-Auto	Auto	Link.
1000-Auto	1000M/Full Fixed	Link unsure. Depends on peer hardware.
1000M/Full Duplex	Auto	Link unsure. Depends on peer hardware.
1000M/Full Duplex	1000M/Full Fixed	Link.

Click **Basic Setting** > **Port Setup** in the navigation panel to display the configuration screen.

Figure 26 Basic Setting > Port Setup


Port Setup
Port
Active
Name
Type
Speed / Duplex
Flow Control
802.1p Priority
BPDU Control
Media Type
* - 1000-Auto 0 Peer sfp_plus
1 1000M/10G 10G / Full Duplex 0 Peer sfp_plus
2 1000M/10G 10G / Full Duplex 0 Peer sfp_plus
3 1000M/10G 10G / Full Duplex 0 Peer sfp_plus
4 1000M/10G 10G / Full Duplex 0 Peer sfp_plus
5 1000M/10G 10G / Full Duplex 0 Peer sfp_plus
6 1000M/10G 10G / Full Duplex 0 Peer sfp_plus
7 1000M/10G 10G / Full Duplex 0 Peer sfp_plus
8 1000M/10G 10G / Full Duplex 0 Peer sfp_plus
9 1000M/10G 10G / Full Duplex 0 Peer sfp_plus
10 1000M/10G 10G / Full Duplex 0 Peer sfp_plus
11 1000M/10G 10G / Full Duplex 0 Peer sfp_plus
12 1000M/10G 10G / Full Duplex 0 Peer sfp_plus
13 1000M/10G 10G / Full Duplex 0 Peer sfp_plus

The following table describes the labels in this screen.

Table 18 Basic Setting > Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	Type a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters. Note: Due to space limitations, the port name may be truncated in some web configurator screens.
Type	This field displays **1000M/10G** for a 1000Base-X connection or 10 Gigabit Ethernet connection, or **40G** for a 40 Gigabit Ethernet connection.
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. The choices are: • **1000-Auto** - use if peer is set as auto-negotiable • **1000M/Full Duplex** - use if peer is set as the same settings (1000Base-X, 1Gbps, full duplex) • **10G/Full Duplex** - use if peer is set at 10Gbps, full duplex. • **40G/Full Duplex** - use if peer is set at 40Gbps, full duplex.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing frame discards and frame losses. **Flow Control** is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE 802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE 802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of frame collision) causing the sending port to temporarily stop sending signals and resend later. Select **Flow Control** to enable it.
802.1p Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See **Priority Queue Assignment** in Table 15 on page 74 for more information.
BPDU Control	Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency in the **Switch Setup** screen first. Select **Peer** to process any BPDU (Bridge Protocol Data Units) received on this port. Select **Tunnel** to forward BPDUs received on this port. Select **Discard** to drop any BPDU received on this port. Select **Network** to process a BPDU with no VLAN tag and forward a tagged BPDU.
Media Type	On any 10 Gigabit interface, such as the SFP+ slot, you can insert either an SFP+ transceiver or an SFP+ Direct Attach Copper (DAC). An SFP+ Direct Attach Copper (DAC) is an SFP+ housing that has no optical module but uses a fixed-length passive copper cable assembly, which reduces cost and power significantly. Select the media type (**sfp_plus** or **dac10g**) of the SFP+ module that is attached to the 10 Gigabit interface.

Table 18 Basic Setting > Port Setup (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

7

VLAN

The type of screen you see here depends on the **VLAN Type** you selected in the **Switch Setup** screen. This chapter shows you how to configure 802.1Q tagged and port-based VLANs.

7.1 Introduction to IEEE 802.1Q Tagged VLANs

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes for the TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes for the TCI (Tag Control Information, starting after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and the value 4095 (FFF) is reserved, so the maximum possible number of VLAN configurations is 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 bits

7.1.1 Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the Switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the Switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

7.2 Automatic VLAN Registration

GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

7.2.1 GARP

GARP (Generic Attribute Registration Protocol) allows network switches to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP.

7.2.1.1 GARP Timers

Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values.

7.2.2 GVRP

GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Enable this function to permit VLAN groups beyond the local Switch.

Please refer to the following table for common IEEE 802.1Q VLAN terminology.

Table 19 IEEE 802.1Q VLAN Terminology

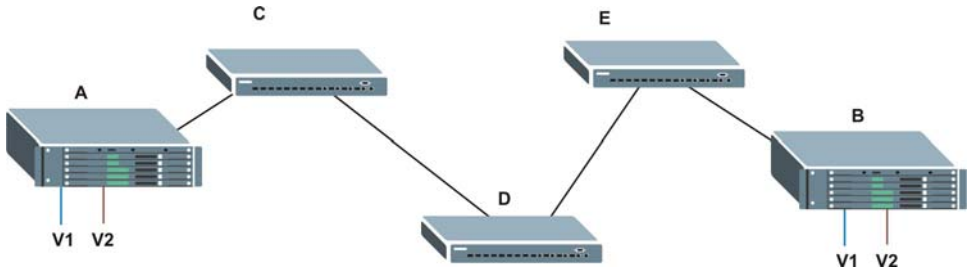
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag Control	Tagged	Ports belonging to the specified VLAN tag all outgoing frames transmitted.
	Untagged	Ports belonging to the specified VLAN don't tag all outgoing frames transmitted.
VLAN Port	Port VID	This is the VLAN ID assigned to untagged frames that this port received.
	Acceptable Frame Type	You may choose to accept both tagged and untagged incoming frames, just tagged incoming frames or just untagged incoming frames on a port.
	Ingress filtering	If set, the Switch discards incoming frames for VLANs that do not have this port as a member.

7.3 Port VLAN Trunking

Enable **VLAN Trunking** on a port to allow frames belonging to unknown VLAN groups to pass through that port. This is useful if you want to set up VLAN groups on end devices without having to configure the same VLAN groups on intermediary devices.

The following figure describes **VLAN Trunking**. Suppose you want to create VLAN groups 1 and 2 (V1 and V2) on devices A and B. Without **VLAN Trunking,** you must configure VLAN groups 1 and 2 on all intermediary switches C, D and E; otherwise they will drop frames with unknown VLAN group tags. However, with **VLAN Trunking** enabled on a port(s) in each intermediary switch you only need to create VLAN groups in the end devices (A and B). C, D and E automatically allow frames with VLAN group tags 1 and 2 (VLAN groups that are unknown to those switches) to pass through their VLAN trunking port(s).

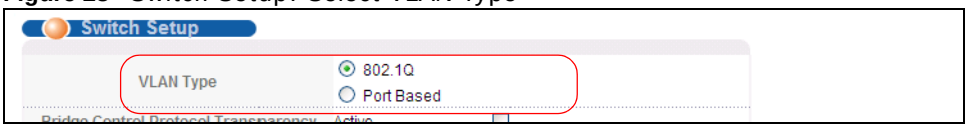
Figure 27 Port VLAN Trunking



7.4 Select the VLAN Type

Select a VLAN type in the **Basic Setting > Switch Setup** screen.

Figure 28 Switch Setup: Select VLAN Type



7.5 802.1Q Static VLAN

Make sure **802.1Q** is selected in the **Basic Setting > Switch Setup** screen.

Use a static VLAN to decide whether an incoming frame on a port should be

- sent to a VLAN group as normal depending on its VLAN tag.
- sent to a group whether it has a VLAN tag or not.
- blocked from a VLAN group regardless of its VLAN tag.

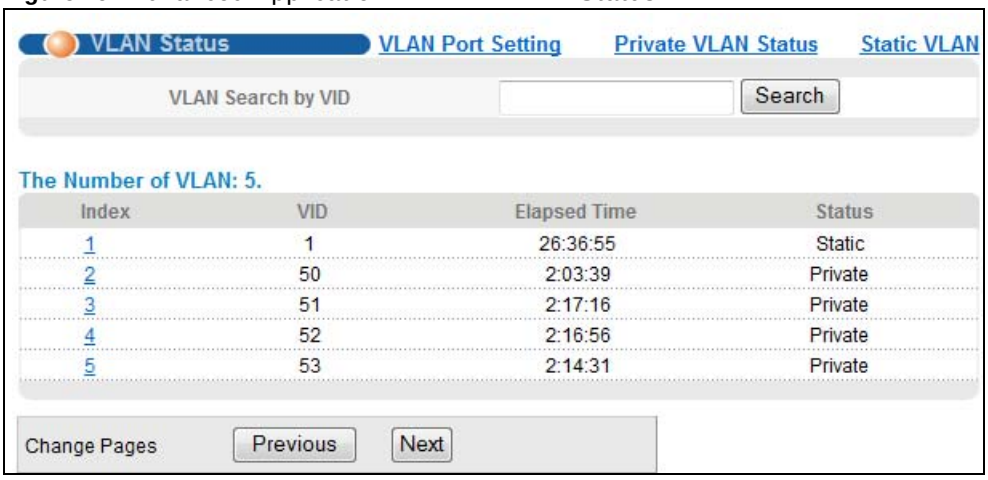
You can also tag all outgoing frames (that were previously untagged) from a port with the specified VID.

You also use the Static VLAN screen to create VLAN IDs for static (normal) or private (primary, isolated or community) VLANs.

7.5.1 VLAN Status

See Section 7.1 on page 81 for more information on 802.1Q VLAN. Click **Advanced Application** > **VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 29 Advanced Application > VLAN: VLAN Status



The following table describes the labels in this screen.

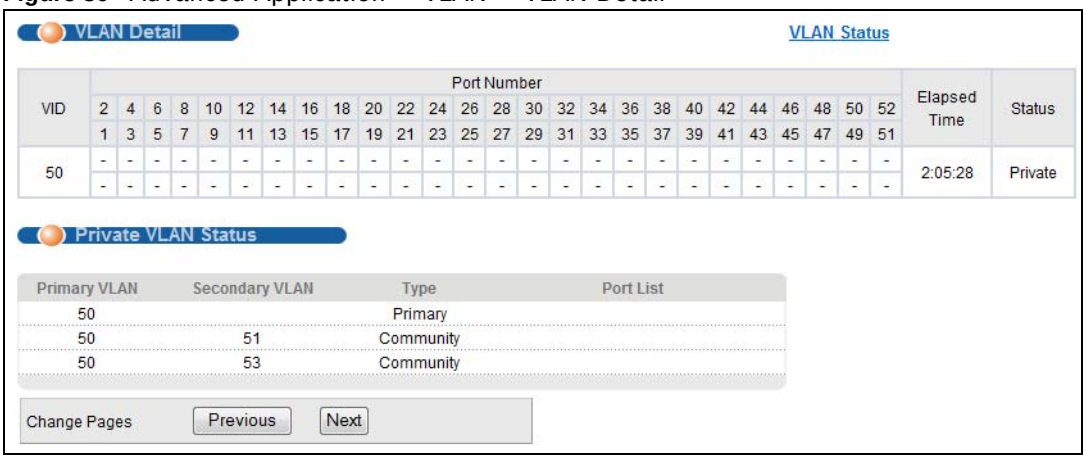
Table 20 Advanced Application > VLAN: VLAN Status

LABEL	DESCRIPTION
VLAN Search by VID	Enter an existing VLAN ID number(s) (separated by a comma) and click **Search** to display only the specified VLAN(s) in the list below. Leave this field blank and click **Search** to display all VLANs configured on the Switch.
The Number of VLAN	This is the number of VLANs configured on the Switch.
The Number of Search Results	This is the number of VLANs that match the searching criteria and display in the list below. This field displays only when you use the **Search** button to look for certain VLANs.
Index	This is the VLAN index number. Click on an index number to view more VLAN details.
VID	This is the VLAN identification number that was configured in the **Static VLAN** screen.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch; • **Dynamic** - using GVRP • **Static** - manually added as a normal entry • **Private** - manually added as a private VLAN (primary, isolated or community) • **MVR** - added via Multicast VLAN Registration (MVR)
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

7.5.2 VLAN Details

Use this screen to view detailed port settings and status of the VLAN group. See Section 7.1 on page 81 for more information on static 802.1Q VLAN. Click on an index number in the **VLAN Status** screen to display VLAN details.

Figure 30 Advanced Application > VLAN > VLAN Detail



The following table describes the labels in this screen.

Table 21 Advanced Application > VLAN > VLAN Detail

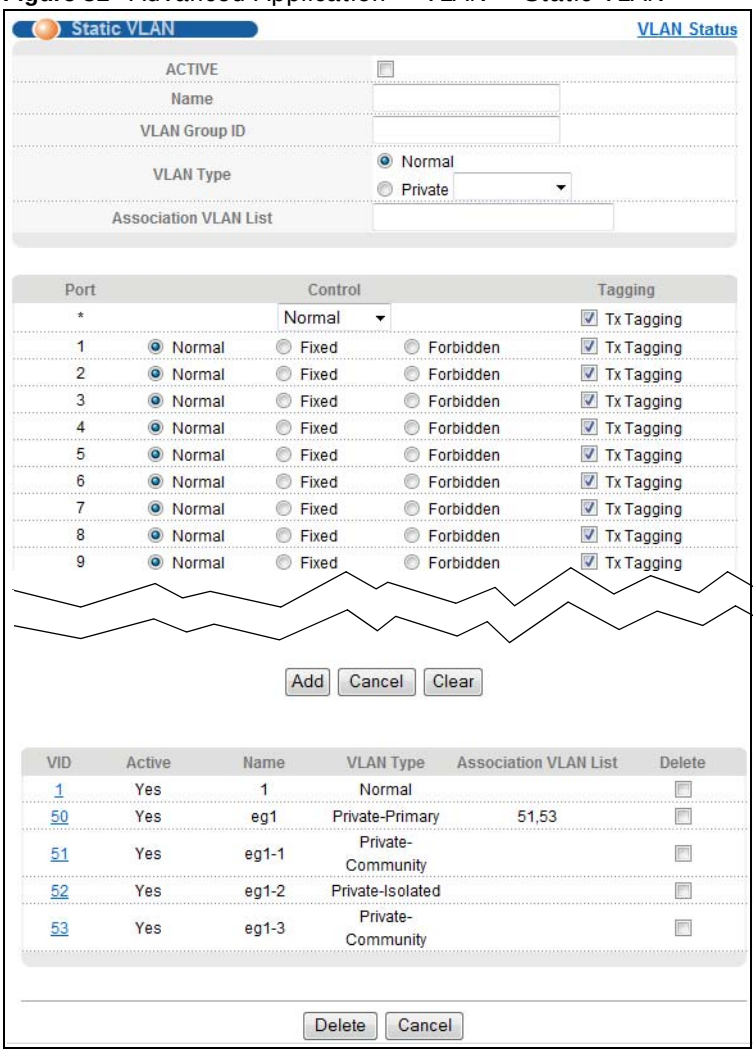
LABEL	DESCRIPTION
VLAN Status	Click this to go to the **VLAN Status** screen.
VLAN Detail	
VID	This is the VLAN identification number that was configured in the **Static VLAN** screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN are marked as "**–**".
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch; • **Dynamic** - using GVRP • **Static** - manually added as a normal entry • **Private** - manually added as a private VLAN (primary, isolated or community) • **MVR** - added via Multicast VLAN Registration (MVR)
Private VLAN Status	These fields show private VLAN information for the selected VLAN. See Chapter 29 on page 236 for more information on private VLANs.
Primary VLAN	This field shows the primary VLAN ID in the selected VLAN.
Secondary VLAN	This field shows the secondary VLAN ID in the selected VLAN.
Type	This field shows the type of private VLAN: **Primary, Community** or **Isolated**.
Port List	This shows the ports mapped to the private VLAN using the **Advanced Application > Private VLAN** or **Advanced Application > VLAN > Static VLAN** screen.
Change Pages	Use the **Previous** and **Next** buttons to display different pages.

7.5.3 Configure a Static VLAN or Private VLAN

Use this screen to create 802.1Q VLAN IDs and set VLAN members for **Normal** (static) or **Private** (**Primary**, **Isolated** or **Community**) VLANs. You must create VLAN IDs for **Private** (**Primary**, **Isolated** or **Community**) VLANs before configuring **Advanced Application > Private VLAN**. See Section 7.1 on page 81 for more information on 802.1Q VLAN.

To configure a static or private VLAN, click **Static VLAN** in the **VLAN Status** screen to display the screen as shown next.

Figure 31 Advanced Application > VLAN > Static VLAN



The following table describes the related labels in this screen.

Table 22 Advanced Application > VLAN > Static VLAN

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.

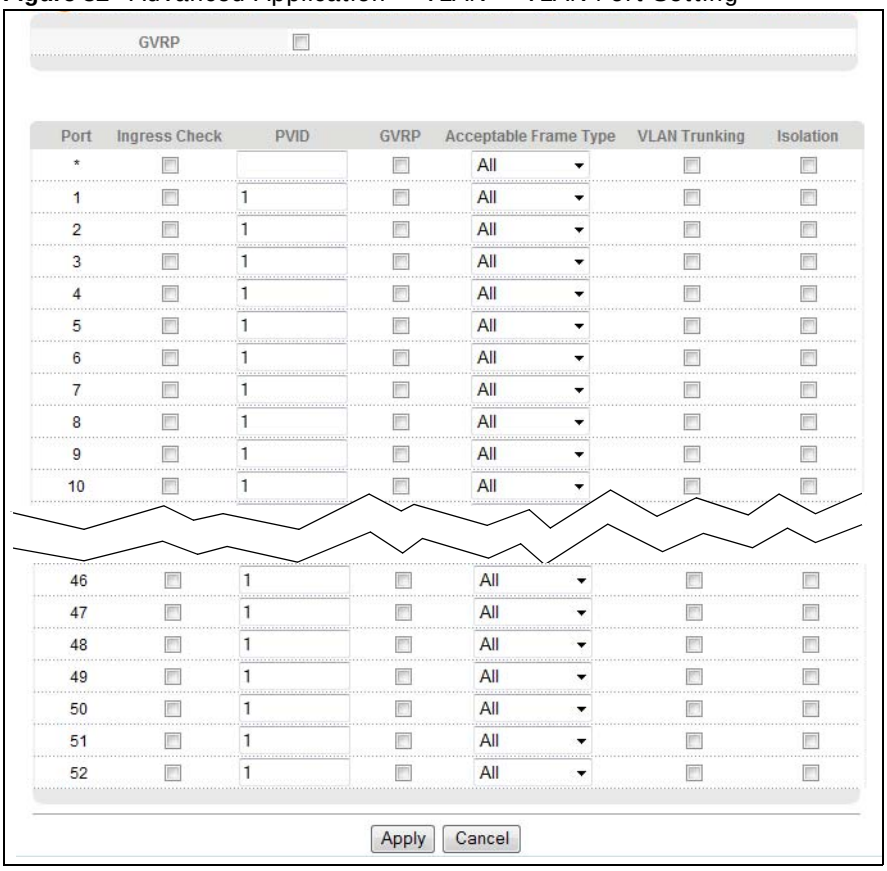
Table 22 Advanced Application > VLAN > Static VLAN (continued)

LABEL	DESCRIPTION
VLAN Type	Select **Normal** (static) or **Private**. For **Private** VLANs, select **Primary**, **Isolated** or **Community**.
Association VLAN List	**Primary** private VLANs can associate with several (secondary) **Community** private VLANs and up to one (secondary) **Isolated** private VLAN. You only configure **VLAN Association List** for **Primary** private VLANs. Use a dash to associate consecutive VLANs and a comma (no spaces) to associate non-consecutive VLANs. For example, 51-53 includes 51, 52 and 53, but 51,53 does not inlcude 52. Secondary private VLANs can only be associated with one primary private VLAN.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Control	Select **Normal** for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select **Fixed** for the port to be a permanent member of this VLAN group. Select **Forbidden** if you want to prohibit the port from joining this VLAN group.
Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (**Yes**) or disabled (**No**).
Name	This field displays the descriptive name for this VLAN group.
VLAN Type	This field displays the **Normal** or **Private** (**Primary**, **Isolated** or **Community**) type VLAN configured in the top part of this screen.
Association VLAN List	This field displays which secondary private VLANs are associated with a primary private VLAN configured in the top part of this screen.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

7.5.4 Configure VLAN Port Settings

Use the VLAN Port Setting screen to configure the static VLAN (IEEE 802.1Q) settings on a port. See Section 7.1 on page 81 for more information on 802.1Q VLAN. Click the **VLAN Port Setting** link in the **VLAN Status** screen.

Figure 32 Advanced Application > VLAN > VLAN Port Setting



The following table describes the labels in this screen.

Table 23 Advanced Application > VLAN > VLAN Port Setting

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Check	If this check box is selected for a port, the Switch discards incoming frames for VLANs that do not include this port in its member set. Clear this check box to disable ingress filtering.

Table 23 Advanced Application > VLAN > VLAN Port Setting (continued)

LABEL	DESCRIPTION
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. Enter a number between 1 and 4094 as the port VLAN ID.
GVRP	Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are **All**, **Tag Only** and **Untag Only**. Select **All** from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select **Tag Only** to accept only tagged frames on this port. All untagged frames will be dropped. Select **Untag Only** to accept only untagged frames on this port. All tagged frames will be dropped.
VLAN Trunking	Enable **VLAN Trunking** on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.
Isolation	Select this to allows this port to communicate only with the CPU management port and the ports on which the isolation feature is not enabled. This has a higher priority than private vlan settings, so promiscuous ports configured in the **Advanced Application > Private VLAN** screen will not be able to communicate with each other if Isolation is selected here.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

7.5.5 Subnet Based VLANs

Subnet based VLANs allow you to group traffic into logical VLANs based on the source IP subnet you specify. When a frame is received on a port, the Switch checks if a tag is added already and the IP subnet it came from. The untagged packets from the same IP subnet are then placed in the same subnet based VLAN. One advantage of using subnet based VLANs is that priority can be assigned to traffic from the same IP subnet.

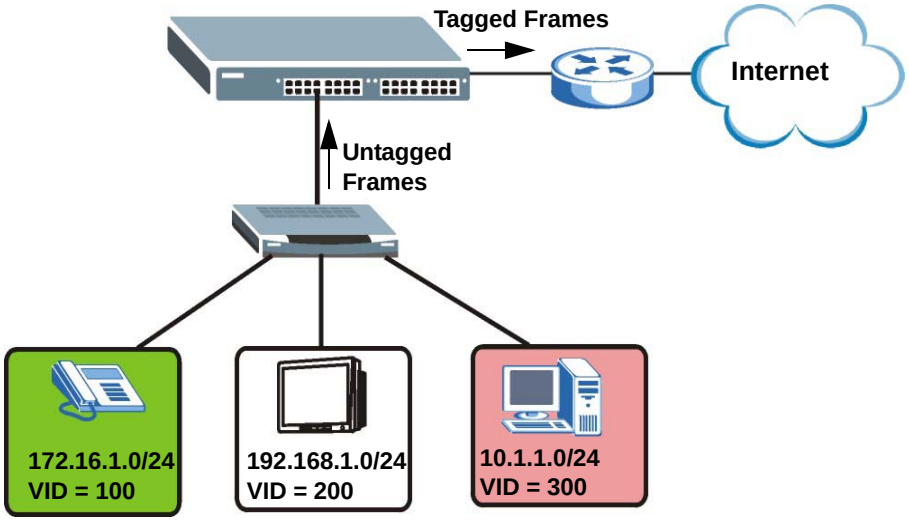
Note: Subnet based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

For example, an ISP (Internet Service Provider) may divide different types of services it provides to customers into different IP subnets. Traffic for voice services is designated for IP subnet 172.16.1.0/24, video for 192.168.1.0/24 and data for 10.1.1.0/24. The Switch can then be configured to group incoming traffic based on the source IP subnet of incoming frames.

You can then configure a subnet based VLAN with priority 6 and VID of 100 for traffic received from IP subnet 172.16.1.0/24 (voice services). You can also have a subnet based VLAN with priority 5 and VID of 200 for traffic received from IP subnet 192.168.1.0/24 (video services). Lastly, you can configure VLAN with priority 3 and VID of 300 for traffic received from IP subnet 10.1.1.0/24 (data

services). All untagged incoming frames will be classified based on their source IP subnet and prioritized accordingly. That is, video services receive the highest priority and data the lowest.

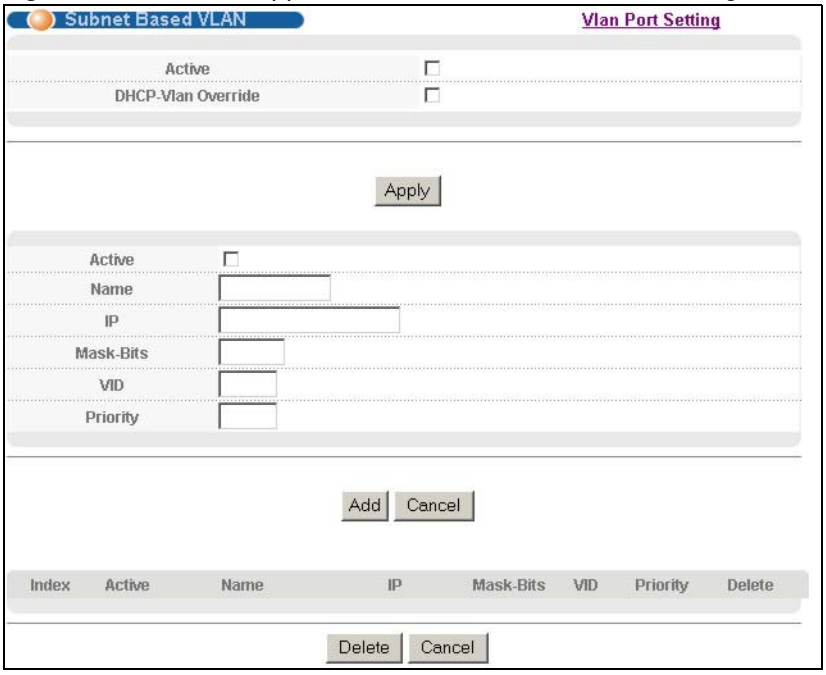
Figure 33 Subnet Based VLAN Application Example



7.5.5.1 Configuring Subnet Based VLAN

Click **Subnet Based VLAN** in the **VLAN Port Setting** screen to display the configuration screen as shown.

Figure 34 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN



The following table describes the labels in this screen.

Table 24 Advanced Application > VLAN > VLAN Port Setting > Subnet Based VLAN Setup

LABEL	DESCRIPTION
Active	Select this check box to activate this subnet based VLANs on the Switch.
DHCP-Vlan Override	When DHCP snooping is enabled DHCP clients can renew their IP address through the DHCP VLAN or via another DHCP server on the subnet based VLAN. Select this checkbox to force the DHCP clients in this IP subnet to obtain their IP addresses through the DHCP VLAN.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Active	Select this check box to activate the IP subnet VLAN you are creating or editing.
Name	Enter up to 32 alphanumeric characters to identify this subnet based VLAN.
IP	Enter the IP address of the subnet for which you want to configure this subnet based VLAN.
Mask-Bits	Enter the bit number of the subnet mask. To find the bit number, convert the subnet mask to binary format and add all the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1s in binary. There are three 255s, so add three eights together and you get the bit number (24).
VID	Enter the ID of a VLAN with which the untagged frames from the IP subnet specified in this subnet based VLAN are tagged. This must be an existing VLAN which you defined in the **Advanced Applications > VLAN** screens.
Priority	Select the priority level that the Switch assigns to frames belonging to this VLAN.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Index	This is the index number identifying this subnet based VLAN. Click on any of these numbers to edit an existing subnet based VLAN.
Active	This field shows whether the subnet based VLAN is active or not.
Name	This field shows the name the subnet based VLAN.
IP	This field shows the IP address of the subnet for this subnet based VLAN.
Mask-Bits	This field shows the subnet mask in bit number format for this subnet based VLAN.
VID	This field shows the VLAN ID of the frames which belong to this subnet based VLAN.
Priority	This field shows the priority which is assigned to frames belonging to this subnet based VLAN.
Delete	Click this to delete the subnet based VLANs which you marked for deletion.
Cancel	Click **Cancel** to begin configuring this screen afresh.

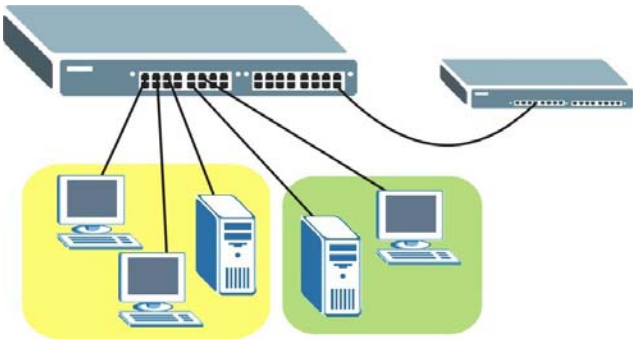
7.5.6 Protocol Based VLANs

Protocol based VLANs allow you to group traffic into logical VLANs based on the protocol you specify. When an upstream frame is received on a port (configured for a protocol based VLAN), the Switch checks if a tag is added already and its protocol. The untagged packets of the same protocol are then placed in the same protocol based VLAN. One advantage of using protocol based VLANs is that priority can be assigned to traffic of the same protocol.

Note: Protocol based VLAN applies to un-tagged packets and is applicable only when you use IEEE 802.1Q tagged VLAN.

For example, ports 1, 2, 3 and 4 belong to static VLAN 100, and ports 4, 5, 6, 7 belong to static VLAN 120. You can configure a protocol based VLAN A with priority 2 for ARP traffic received on port 1, 2 and 3. You can also have a protocol based VLAN B with priority 3 for Apple Talk traffic received on port 6 and 7. All upstream ARP traffic from port 1, 2 and 3 will be grouped together, and all upstream Apple Talk traffic from port 6 and 7 will be in another group and have higher priority than ARP traffic when they go through the uplink port to a backbone switch C.

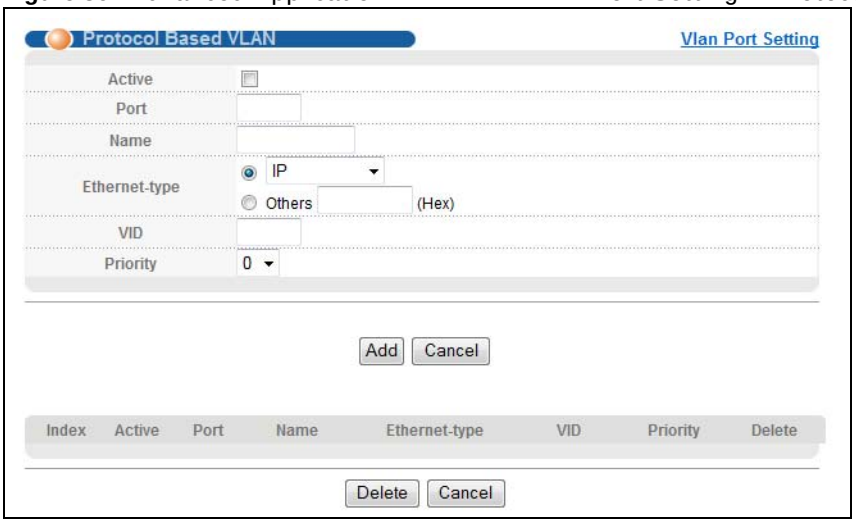
Figure 35 Protocol Based VLAN Application Example



7.5.6.1 Configuring Protocol Based VLAN

Click **Protocol Based VLAN** in the **VLAN Port Setting** screen to display the configuration screen as shown.

Figure 36 Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN



The following table describes the labels in this screen.

Table 25 Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN Setup

LABEL	DESCRIPTION
Active	Select this check box to activate this protocol based VLAN.
Port	Type a port number to be included in this protocol based VLAN. This port must belong to a static VLAN in order to participate in a protocol based VLAN. See Chapter 7 on page 81 for more details on setting up VLANs.
Name	Enter up to 32 alphanumeric characters to identify this protocol based VLAN.

Table 25 Advanced Application > VLAN > VLAN Port Setting > Protocol Based VLAN Setup

LABEL	DESCRIPTION
Ethernet-type	Use the drop down list box to select a predefined protocol to be included in this protocol based VLAN or select **Others** and type the protocol number in hexadecimal notation. For example, the IP protocol in hexadecimal notation is 0800, and Novell IPX protocol is 8137. Note: Protocols in the hexadecimal number range of 0x0000 to 0x05ff are not allowed to be used for protocol based VLANs.
VID	Enter the ID of a VLAN to which the port belongs. This must be an existing VLAN which you defined in the **Advanced Applications > VLAN** screens.
Priority	Select the priority level that the Switch will assign to frames belonging to this VLAN.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Index	This is the index number identifying this protocol based VLAN. Click on any of these numbers to edit an existing protocol based VLAN.
Active	This field shows whether the protocol based VLAN is active or not.
Port	This field shows which port belongs to this protocol based VLAN.
Name	This field shows the name the protocol based VLAN.
Ethernet-type	This field shows which Ethernet protocol is part of this protocol based VLAN.
VID	This field shows the VLAN ID of the port.
Priority	This field shows the priority which is assigned to frames belonging to this protocol based VLAN.
Delete	Click this to delete the protocol based VLANs which you marked for deletion.
Cancel	Click **Cancel** to begin configuring this screen afresh.

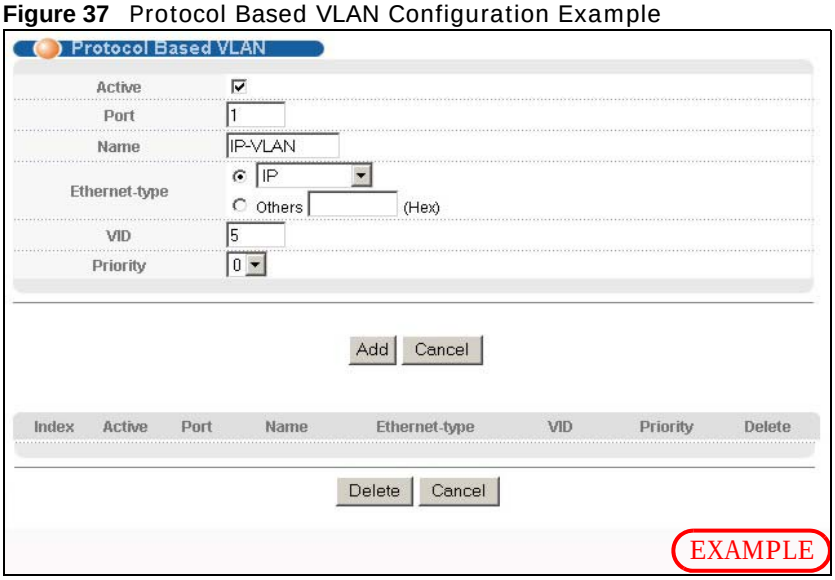
7.5.6.2 Create an IP-based VLAN Example

This example shows you how to create an IP VLAN which includes ports 1, 4 and 8. Follow these steps using the screen below:

1. Activate this protocol based VLAN.
2. Type the port number you want to include in this protocol based VLAN. Type **1**.
3. Give this protocol-based VLAN a descriptive name. Type **IP-VLAN**.
4. Select the protocol. Leave the default value **IP**.
5. Type the VLAN ID of an existing VLAN. In our example we already created a static VLAN with an ID of 5. Type **5**.

6 Leave the priority set to **0** and click **Add**.

Figure 37 Protocol Based VLAN Configuration Example



To add more ports to this protocol based VLAN.

1 Click the index number of the protocol based VLAN entry. Click **1**

2 Change the value in the **Port** field to the next port you want to add.

3 Click **Add**.

7.5.7 View Private VLAN Status

Use this screen to view all private VLANs created on the Switch. See also **Advanced Application > Private VLAN**.

Make sure **802.1Q** is selected in the **Basic Setting > Switch Setup** screen.

Click **Private VLAN Status** in the **VLAN Status** screen to display the screen as shown next.

Figure 38 Advanced Application > VLAN > Private VLAN Status

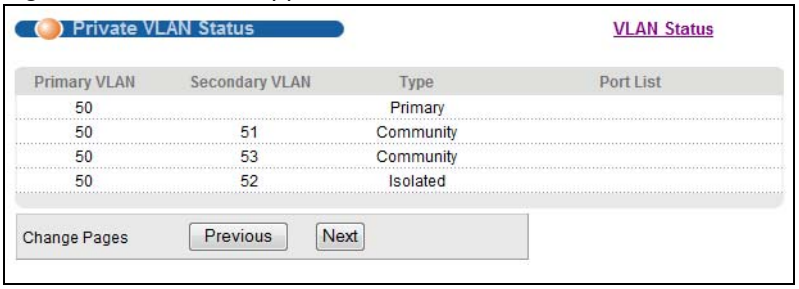


Table 26 Advanced Application > VLAN > Private VLAN Status

LABEL	DESCRIPTION
Private VLAN Status	These fields show information for the all private VLANs. See also **Advanced Application > Private VLAN**.
Primary VLAN	This field shows the primary VLAN ID in a private VLAN.
Secondary VLAN	This field shows the secondary VLAN ID in a private VLAN.
Type	This field shows the type of private VLAN: **Primary, Community** or **Isolated**.
Port List	This shows the ports mapped to the private VLAN using the **Advanced Application > Private VLAN** or **Advanced Application > VLAN > Static VLAN** screen.
Change Pages	Use the **Previous** and **Next** buttons to display different pages.

7.6 Port-based VLAN Setup

Port-based VLANs are VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

Port-based VLANs require allowed outgoing ports to be defined for each port. Therefore, if you wish to allow two subscriber ports to talk to each other, for example, between conference rooms in a hotel, you must define the egress (an egress port is an outgoing port, that is, a port through which a data packet leaves) for both ports.

Port-based VLANs are specific only to the Switch on which they were created.

Note: When you activate port-based VLAN, the Switch uses a default VLAN ID of 1. You cannot change it.

Note: In screens (such as **IP Setup** and **Filtering**) that require a VID, you must enter 1 as the VID.

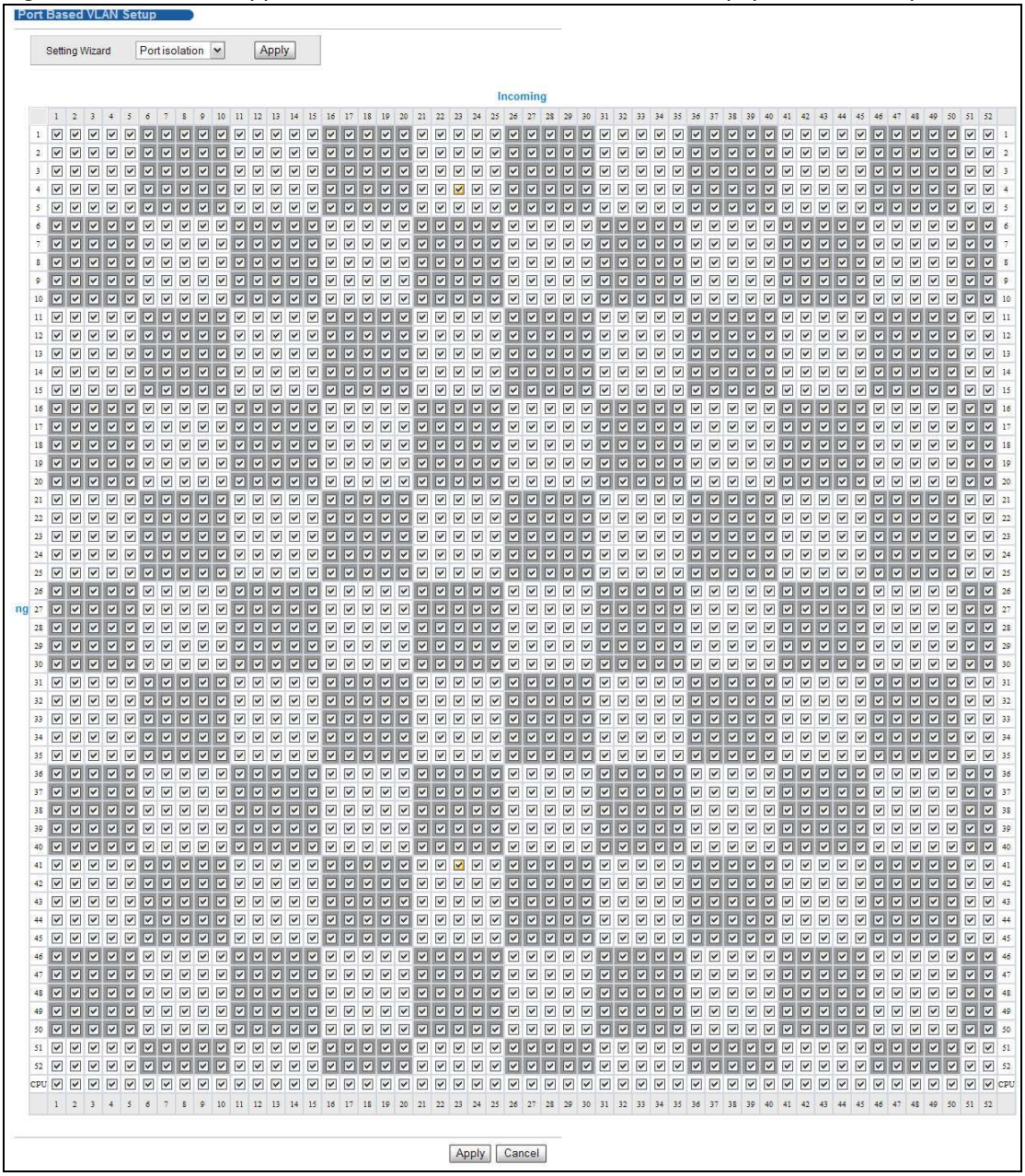
The port-based VLAN setup screen is shown next. The **CPU** management port forms a VLAN with all Ethernet ports.

7.6.1 Configure a Port-based VLAN

Select **Port Based** as the **VLAN Type** in the **Switch Setup** screen and then click **VLAN** from the navigation panel to display the following screen. Select either **All Connected** or **Port Isolated** from the drop-down list depending on your VLAN and VLAN security requirements. If VLAN members need to communicate directly with each other, then select **All Connected**. Select **Port Isolated** if you want to restrict users from communicating directly. Click **Apply** to save your settings.

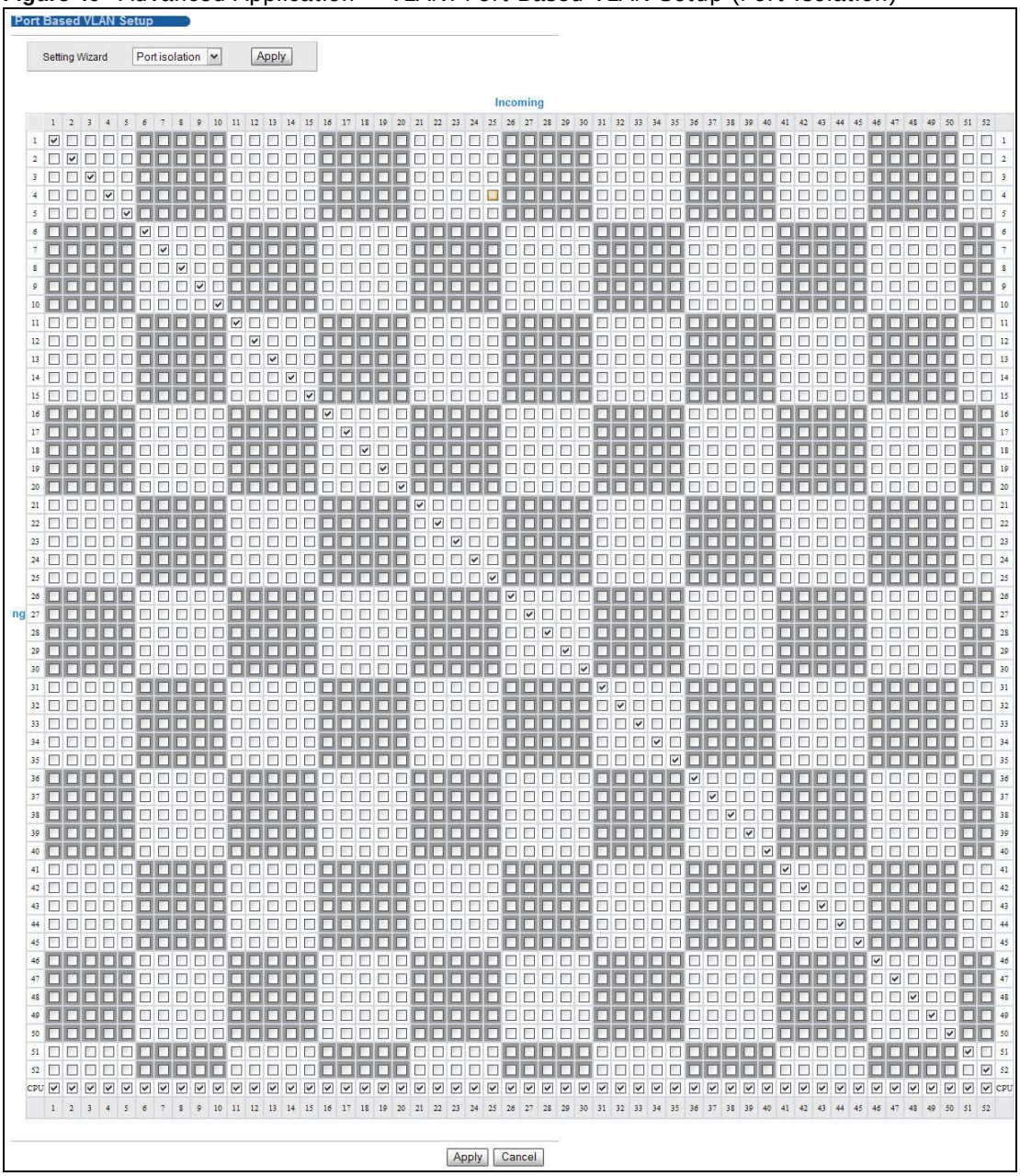
The following screen shows users on a port-based, all-connected VLAN configuration.

Figure 39 Advanced Application > VLAN > Port Based VLAN Setup (All Connected)



The following screen shows users on a port-based, port-isolated VLAN configuration.

Figure 40 Advanced Application > VLAN: Port Based VLAN Setup (Port Isolation)



The following table describes the labels in this screen.

Table 27 Advanced Application > VLAN: Port Based VLAN Setup

LABEL	DESCRIPTION
Setting Wizard	Choose **All connected** or **Port isolation**. **All connected** means all ports can communicate with each other, that is, there are no virtual LANs. All incoming and outgoing ports are selected. This option is the most flexible but also the least secure. **Port isolation** means that each port can only communicate with the CPU management port and cannot communicate with each other. All incoming ports are selected while only the CPU outgoing port is selected. This option is the most limiting but also the most secure. After you make your selection, click **Apply** (top right of screen) to display the screens as mentioned above. You can still customize these settings by adding/deleting incoming or outgoing ports, but you must also click **Apply** at the bottom of the screen.
Incoming	These are the ingress ports; an ingress port is an incoming port, that is, a port through which a data packet enters. If you wish to allow two subscriber ports to talk to each other, you must define the ingress port for both ports. The numbers in the top row denote the incoming port for the corresponding port listed on the left (its outgoing port). **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.
Outgoing	These are the egress ports. An egress port is an outgoing port, that is, a port through which a data packet leaves. If you wish to allow two subscriber ports to talk to each other, you must define the egress port for both ports. **CPU** refers to the Switch management port. By default it forms a VLAN with all Ethernet ports. If it does not form a VLAN with a particular port then the Switch cannot be managed from that port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8

Static MAC Forward Setup

Use these screens to configure static MAC address forwarding.

8.1 Overview

This chapter discusses how to configure forwarding rules based on MAC addresses of devices on your network.

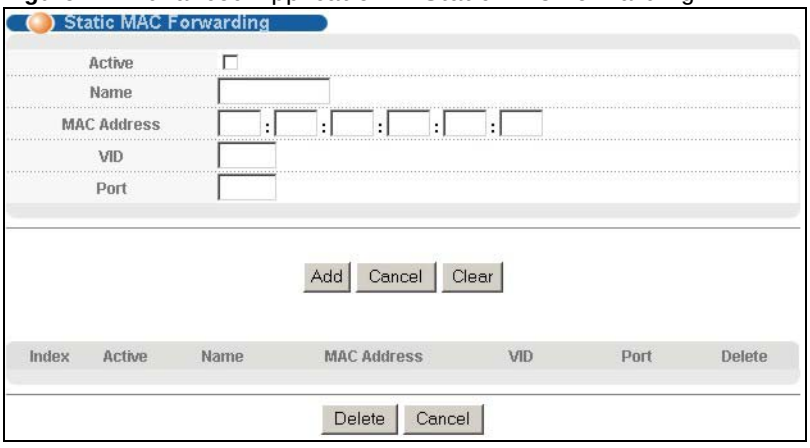
8.2 Configuring Static MAC Forwarding

A static MAC address is an address that has been manually entered in the MAC address table. Static MAC addresses do not age out. When you set up static MAC address rules, you are setting static MAC addresses for a port. This may reduce the need for broadcasting.

Static MAC address forwarding together with port security allows only computers in the MAC address table on a port to access the Switch. See Chapter 17 on page 148 for more information on port security.

Click **Advanced Applications > Static MAC Forwarding** in the navigation panel to display the configuration screen as shown.

Figure 41 Advanced Application > Static MAC Forwarding



The following table describes the labels in this screen.

Table 28 Advanced Application > Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port	Enter the port where the MAC address entered in the previous field will be automatically forwarded.
Add	Click **Add** to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (**Yes**) or not (**No**). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the ID number of the VLAN group.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

9

Static Multicast Forward Setup

Use these screens to configure static multicast address forwarding.

9.1 Static Multicast Forwarding Overview

A multicast MAC address is the MAC address of a member of a multicast group. A static multicast address is a multicast MAC address that has been manually entered in the multicast table. Static multicast addresses do not age out. Static multicast forwarding allows you (the administrator) to forward multicast frames to a member without the member having to join the group first.

If a multicast group has no members, then the switch will either flood the multicast frames to all ports or drop them. You can configure this in the **Advanced Application** > **Multicast** > **Multicast Setting** screen (see Section 22.3 on page 174). Figure 42 shows such unknown multicast frames flooded to all ports. With static multicast forwarding, you can forward these multicasts to port(s) within a VLAN group. Figure 43 shows frames being forwarded to devices connected to port 3. Figure 44 shows frames being forwarded to ports 2 and 3 within VLAN group 4.

Figure 42 No Static Multicast Forwarding

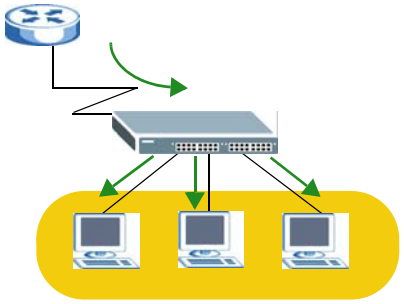


Figure 43 Static Multicast Forwarding to A Single Port

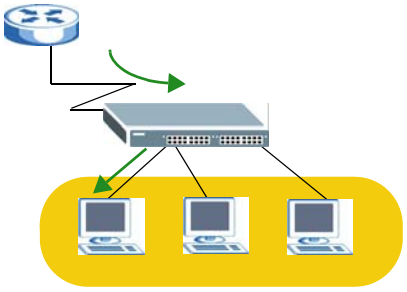
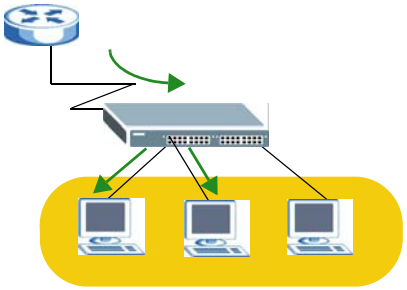


Figure 44 Static Multicast Forwarding to Multiple Ports

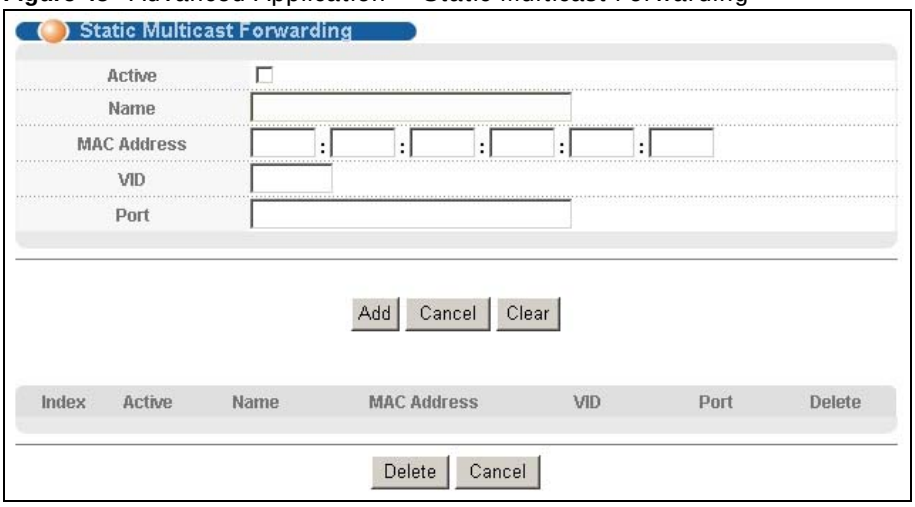


9.2 Configuring Static Multicast Forwarding

Use this screen to configure rules to forward specific multicast frames, such as streaming or control frames, to specific port(s).

Click **Advanced Application** > **Static Multicast Forwarding** to display the configuration screen as shown.

Figure 45 Advanced Application > Static Multicast Forwarding



The following table describes the labels in this screen.

Table 29 Advanced Application > Static Multicast Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this static multicast MAC address forwarding rule. This is for identification only.
MAC Address	Enter a multicast MAC address which identifies the multicast group. The last binary bit of the first octet pair in a multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 and 00000011 is 03 in hexadecimal, so 01:00:5e:00:00:0A and 03:00:5e:00:00:27 are valid multicast MAC addresses.
VID	You can forward frames with matching destination MAC address to port(s) within a VLAN group. Enter the ID that identifies the VLAN group here. If you don't have a specific target VLAN, enter 1.
Port	Enter the port(s) where frames with destination MAC address that matched the entry above are forwarded. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Add	Click **Add** to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to their last saved values.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	Click an index number to modify a static multicast MAC address rule for port(s).
Active	This field displays whether a static multicast MAC address forwarding rule is active (**Yes**) or not (**No**). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for a static multicast MAC address-forwarding rule.
MAC Address	This field displays the multicast MAC address that identifies a multicast group.
VID	This field displays the ID number of a VLAN group to which frames containing the specified multicast MAC address will be forwarded.

Table 29 Advanced Application > Static Multicast Forwarding (continued)

LABEL	DESCRIPTION
Port	This field displays the port(s) within a identified VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

10

Filtering

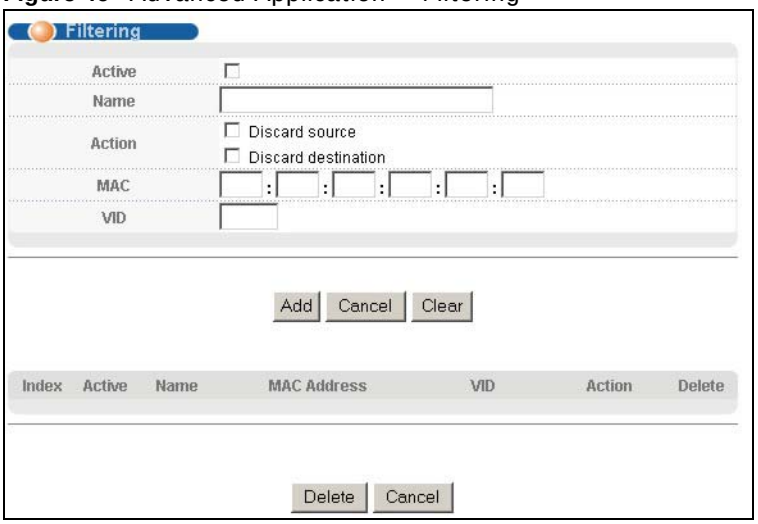
This chapter discusses MAC address port filtering.

10.1 Configure a Filtering Rule

Configure the Switch to filter traffic based on the traffic's source, destination MAC addresses and/or VLAN group (ID).

Click **Advanced Application** > **Filtering** in the navigation panel to display the screen as shown next.

Figure 46 Advanced Application > Filtering



The following table describes the related labels in this screen.

Table 30 Advanced Application > FIltering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification only.
Action	Select **Discard source** to drop frames from the source MAC address (specified in the **MAC** field). The Switch can still send frames to the MAC address. Select **Discard destination** to drop frames to the destination MAC address (specified in the **MAC** address). The Switch can still receive frames originating from the MAC address. Select **Discard source** and **Discard destination** to block traffic to/from the MAC address specified in the **MAC** field.

Table 30 Advanced Application > FIltering (continued)

LABEL	DESCRIPTION
MAC	Type a MAC address in a valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays **Yes** when the rule is activated and **No** when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purposes only.
MAC Address	This field displays the source/destination MAC address with the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN group identification number.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es) in the **Delete** column.

11

Spanning Tree Protocol

The Switch supports Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) as defined in the following standards.

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w Rapid Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree Protocol

The Switch also allows you to set up multiple STP configurations (or trees). Ports can then be assigned to the trees.

11.1 STP/RSTP Overview

(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a Switch to interact with other (R)STP-compliant switches in your network to ensure that only one path exists between any two stations on the network.

The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the spanning tree than STP (while also being backwards compatible with STP-only aware bridges). In RSTP, topology change information is directly propagated throughout the network from the device that generates the topology change. In STP, a longer delay is required as the device that causes a topology change first notifies the root bridge and then the root bridge notifies the network. Both RSTP and STP flush unwanted learned addresses from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

Note: In this user's guide, "STP" refers to both STP and RSTP.

11.1.1 STP Terminology

The root bridge is the base of the spanning tree.

Path cost is the cost of transmitting a frame onto a LAN through that port. The recommended cost is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost.

Table 31 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535

Table 31 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the bridge communicates with the root through the root port. The root port is the port on this Switch with the lowest path cost to the root (the root path cost). If there is no root port, then this Switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

11.1.2 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware switches exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

11.1.3 STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 32 STP Port States

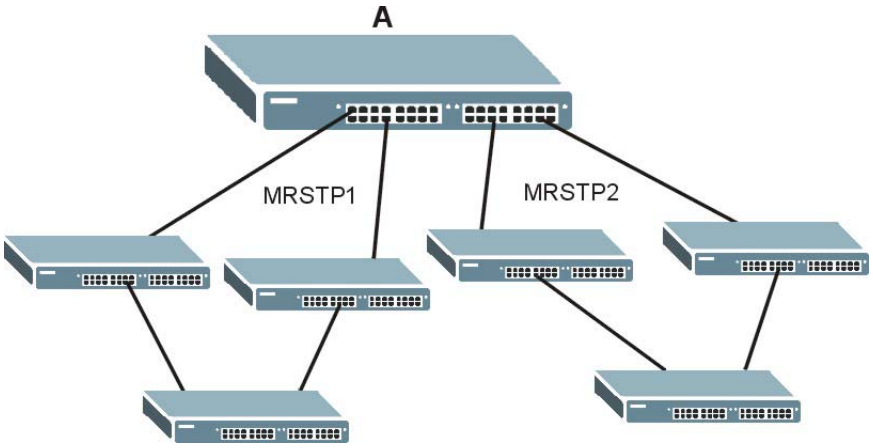
PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed. Note: The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

11.1.4 Multiple RSTP

MRSTP (Multiple RSTP) is ZyXEL's proprietary feature that is compatible with RSTP and STP. With MRSTP, you can have more than one spanning tree on your Switch and assign port(s) to each tree. Each spanning tree operates independently with its own bridge information.

In the following example, there are two RSTP instances (**MRSTP 1** and **MRSTP2**) on switch **A**.

Figure 47 MRSTP Network Example



To set up MRSTP, activate MRSTP on the Switch and specify which port(s) belong to which spanning tree.

Note: Each port can belong to one STP tree only.

11.1.5 Multiple STP

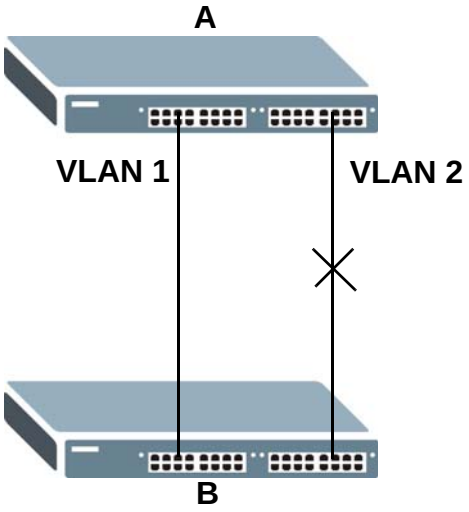
Multiple Spanning Tree Protocol (IEEE 802.1s) is backwards compatible with STP/RSTP and addresses the limitations of existing spanning tree protocols (STP and RSTP) in networks to include the following features:

- One Common and Internal Spanning Tree (CIST) that represents the entire network's connectivity.
- Grouping of multiple bridges (or switching devices) into regions that appear as one single bridge on the network.
- A VLAN can be mapped to a specific Multiple Spanning Tree Instance (MSTI). MSTI allows multiple VLANs to use the same spanning tree.
- Load-balancing is possible as traffic from different VLANs can use distinct paths in a region.

11.1.5.1 MSTP Network Example

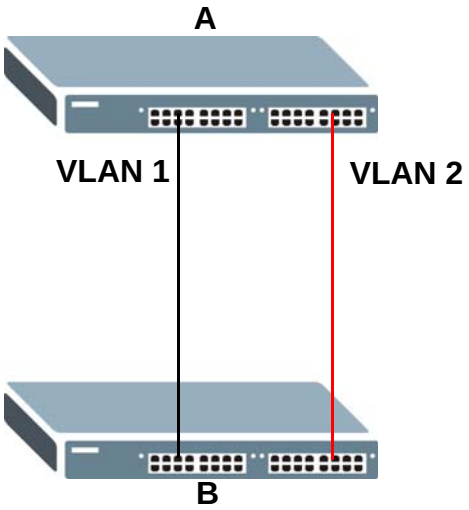
The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 2 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

Figure 48 STP/RSTP Network Example



With MSTP, VLANs 1 and 2 are mapped to different spanning trees in the network. Thus traffic from the two VLANs travel on different paths. The following figure shows the network example using MSTP.

Figure 49 MSTP Network Example



11.1.5.2 MST Region

An MST region is a logical grouping of multiple network devices that appears as a single device to the rest of the network. Each MSTP-enabled device can only belong to one MST region. When BPDUs enter an MST region, external path cost (of paths outside this region) is increased by one. Internal path cost (of paths within this region) is increased by one when BPDUs traverse the region.

Devices that belong to the same MST region are configured to have the same MSTP configuration identification settings. These include the following parameters:

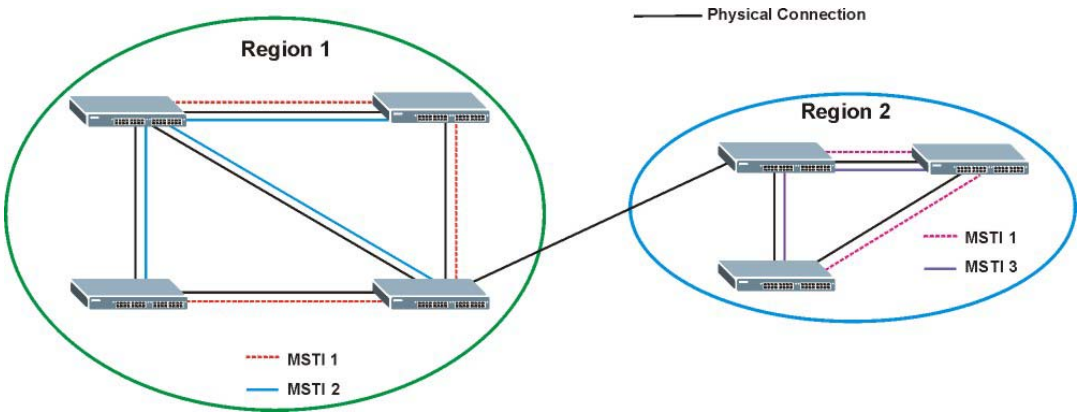
- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

11.1.5.3 MST Instance

An MST Instance (MSTI) is a spanning tree instance. VLANs can be configured to run on a specific MSTI. Each created MSTI is identified by a unique number (known as an MST ID) known internally to a region. Thus an MSTI does not span across MST regions.

The following figure shows an example where there are two MST regions. Regions 1 and 2 have 2 spanning tree instances.

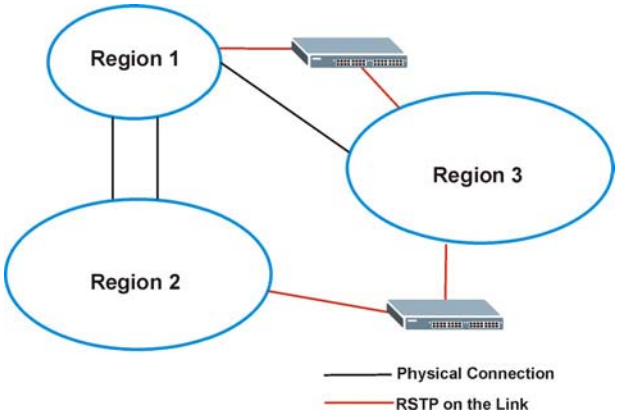
Figure 50 MSTIs in Different Regions



11.1.5.4 Common and Internal Spanning Tree (CIST)

A CIST represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/RSTP. The CIST is the default MST instance (MSTID 0). Any VLANs that are not members of an MST instance are members of the CIST. In an MSTP-enabled network, there is only one CIST that runs between MST regions and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP.

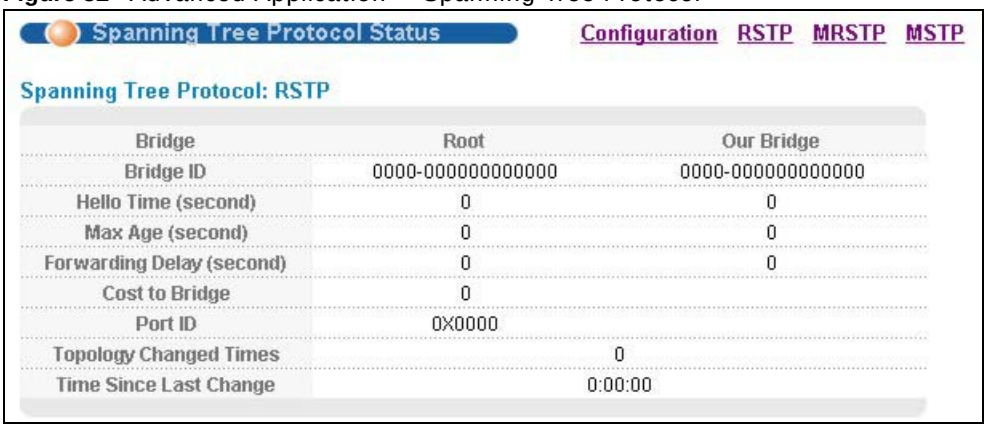
Figure 51 MSTP and Legacy RSTP Network Example



11.2 Spanning Tree Protocol Status Screen

The Spanning Tree Protocol status screen changes depending on what standard you choose to implement on your network. Click **Advanced Application** > **Spanning Tree Protocol** to see the screen as shown.

Figure 52 Advanced Application > Spanning Tree Protocol



This screen differs depending on which STP mode (RSTP, MRSTP or MSTP) you configure on the Switch. This screen is described in detail in the section that follows the configuration section for each STP mode. Click **Configuration** to activate one of the STP standards on the Switch.

11.3 Spanning Tree Configuration

Use the **Spanning Tree Configuration** screen to activate one of the STP modes on the Switch. Click **Configuration** in the **Advanced Application** > **Spanning Tree Protocol**.

Figure 53 Advanced Application > Spanning Tree Protocol > Configuration

The following table describes the labels in this screen.

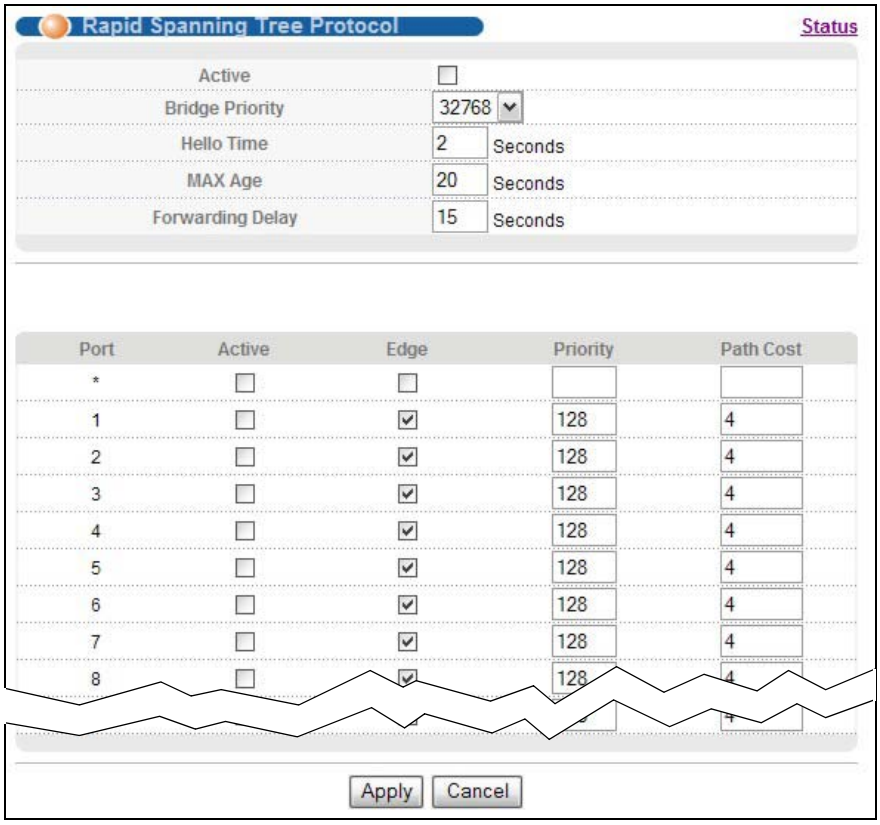
Table 33 Advanced Application > Spanning Tree Protocol > Configuration

LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the Switch. Select **Rapid Spanning Tree**, **Multiple Rapid Spanning Tree** or **Multiple Spanning Tree**. See Section 11.1 on page 107 for background information on STP.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.4 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see Section 11.1 on page 107 for more information on RSTP. Click **RSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen.

Figure 54 Advanced Application > Spanning Tree Protocol > RSTP



The following table describes the labels in this screen.

Table 34 Advanced Application > Spanning Tree Protocol > RSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **RSTP Status** screen (see Figure 55 on page 115).
Active	Select this check box to activate RSTP. Clear this checkbox to disable RSTP. Note: You must also activate **Rapid Spanning Tree** in the **Advanced Application** > **Spanning Tree Protocol** > **Configuration** screen to enable RSTP on the Switch.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.

Table 34 Advanced Application > Spanning Tree Protocol > RSTP (continued)

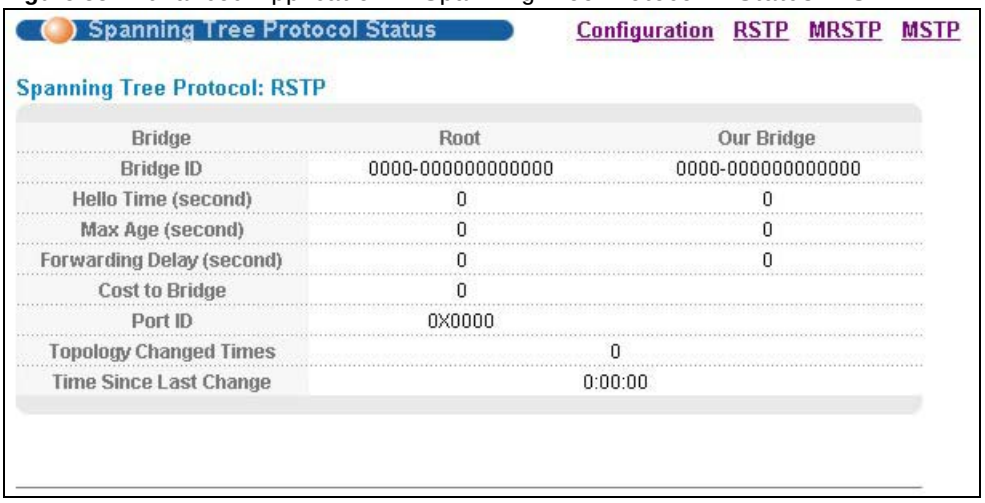
LABEL	DESCRIPTION
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate RSTP on this port.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 31 on page 107 for more information.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.5 Rapid Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 11.1 on page 107 for more information on RSTP.

Note: This screen is only available after you activate RSTP on the Switch.

Figure 55 Advanced Application > Spanning Tree Protocol > Status: RSTP



The following table describes the labels in this screen.

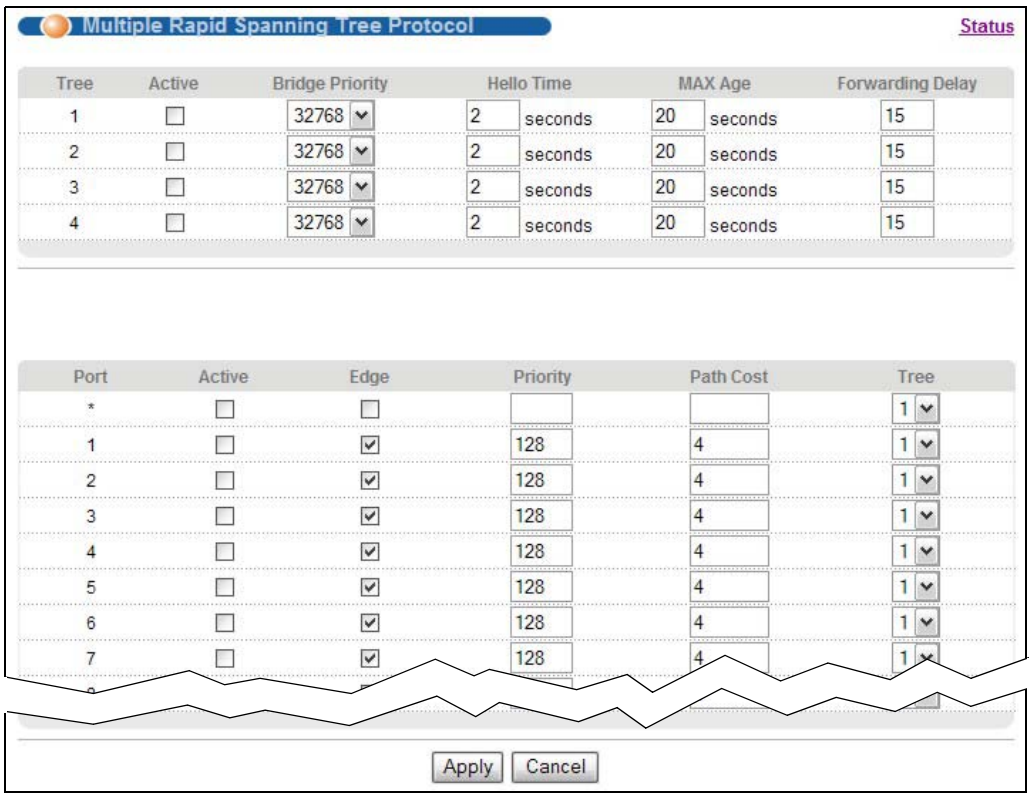
Table 35 Advanced Application > Spanning Tree Protocol > Status: RSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **RSTP** to edit RSTP settings on the Switch.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of the bridge priority plus the MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). See Section 11.1.3 on page 108 for information on port states. Note: The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

11.6 Configure Multiple Rapid Spanning Tree Protocol

To configure MRSTP, click **MRSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen. See Section 11.1 on page 107 for more information on MRSTP.

Figure 56 Advanced Application > Spanning Tree Protocol > MRSTP



The following table describes the labels in this screen.

Table 36 Advanced Application > Spanning Tree Protocol > MRSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **MRSTP Status** screen (see Figure 55 on page 115).
Tree	This is a read only index number of the STP trees.
Active	Select this check box to activate an STP tree. Clear this checkbox to disable an STP tree. Note: You must also activate **Multiple Rapid Spanning Tree** in the **Advanced Application** > **Spanning Tree Protocol** > **Configuration** screen to enable MRSTP on the Switch.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.

Table 36 Advanced Application > Spanning Tree Protocol > MRSTP (continued)

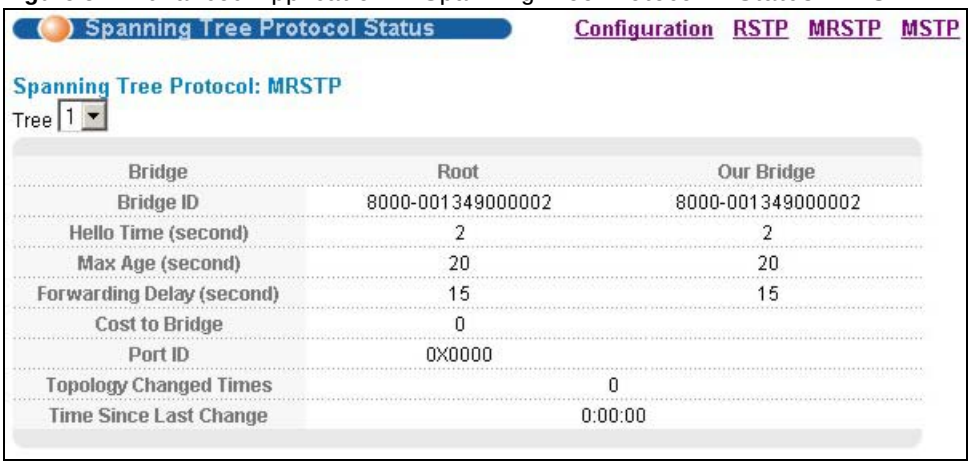
LABEL	DESCRIPTION
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate STP on this port.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in the Switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended that you assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 31 on page 107 for more information.
Tree	Select which STP tree configuration this port should participate in.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.7 Multiple Rapid Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 11.1 on page 107 for more information on MRSTP.

Note: This screen is only available after you activate MRSTP on the Switch.

Figure 57 Advanced Application > Spanning Tree Protocol > Status: MRSTP



The following table describes the labels in this screen.

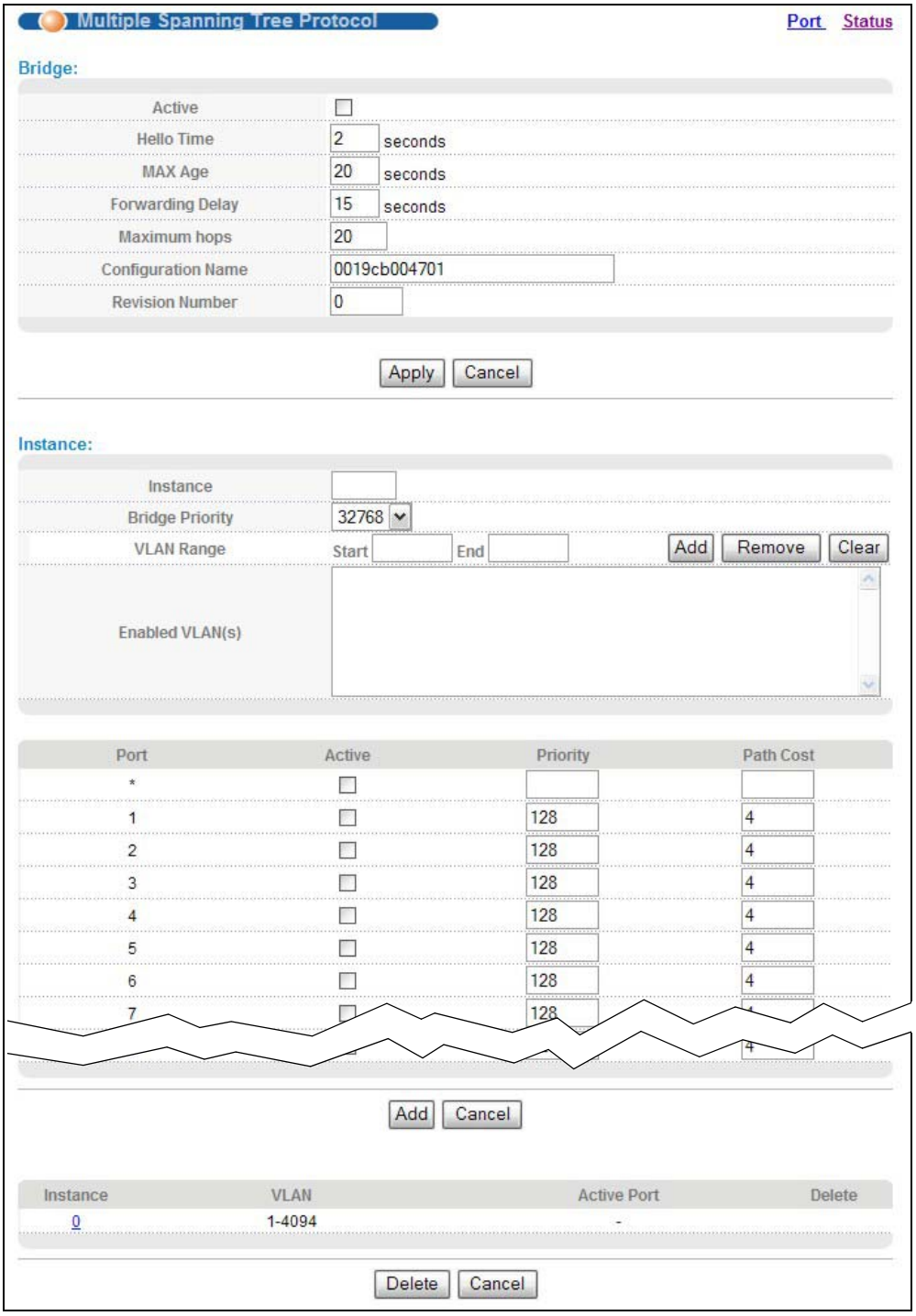
Table 37 Advanced Application > Spanning Tree Protocol > Status: MRSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **MRSTP** to edit MRSTP settings on the Switch.
Tree	Select which STP tree configuration you want to view.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.

11.8 Configure Multiple Spanning Tree Protocol

To configure MSTP, click **MSTP** in the **Advanced Application** > **Spanning Tree Protocol** screen. See Section 11.1.5 on page 109 for more information on MSTP.

Figure 58 Advanced Application > Spanning Tree Protocol > MSTP



The following table describes the labels in this screen.

Table 38 Advanced Application > Spanning Tree Protocol > MSTP

LABEL	DESCRIPTION
Status	Click **Status** to display the **MSTP Status** screen (see Figure 60 on page 123).
Active	Select this check box to activate MSTP on the Switch. Clear this checkbox to disable MSTP on the Switch. Note: You must also activate **Multiple Spanning Tree** in the **Advanced Application > Spanning Tree Protocol > Configuration** screen to enable MSTP on the Switch.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
MaxAge	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Maximum hops	Enter the number of hops (between 1 and 255) in an MSTP region before the BPDU is discarded and the port information is aged.
Configuration Name	Enter a descriptive name (up to 32 characters) of an MST region.
Revision Number	Enter a number to identify a region's configuration. Devices must have the same revision number to belong to the same region.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Instance	Use this section to configure MSTI (Multiple Spanning Tree Instance) settings.
Instance	Enter the number you want to use to identify this MST instance on the Switch. The Switch supports instance numbers 0-16.
Bridge Priority	Set the priority of the Switch for the specific spanning tree instance. The lower the number, the more likely the Switch will be chosen as the root bridge within the spanning tree instance. Enter priority values between 0 and 61440 in increments of 4096 (thus valid values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440).
VLAN Range	Enter the start of the VLAN ID range that you want to add or remove from the VLAN range edit area in the **Start** field. Enter the end of the VLAN ID range that you want to add or remove from the VLAN range edit area in the **End** field. Next click: • **Add** - to add this range of VLAN(s) to be mapped to the MST instance. • **Remove** - to remove this range of VLAN(s) from being mapped to the MST instance. • **Clear** - to remove all VLAN(s) from being mapped to this MST instance.

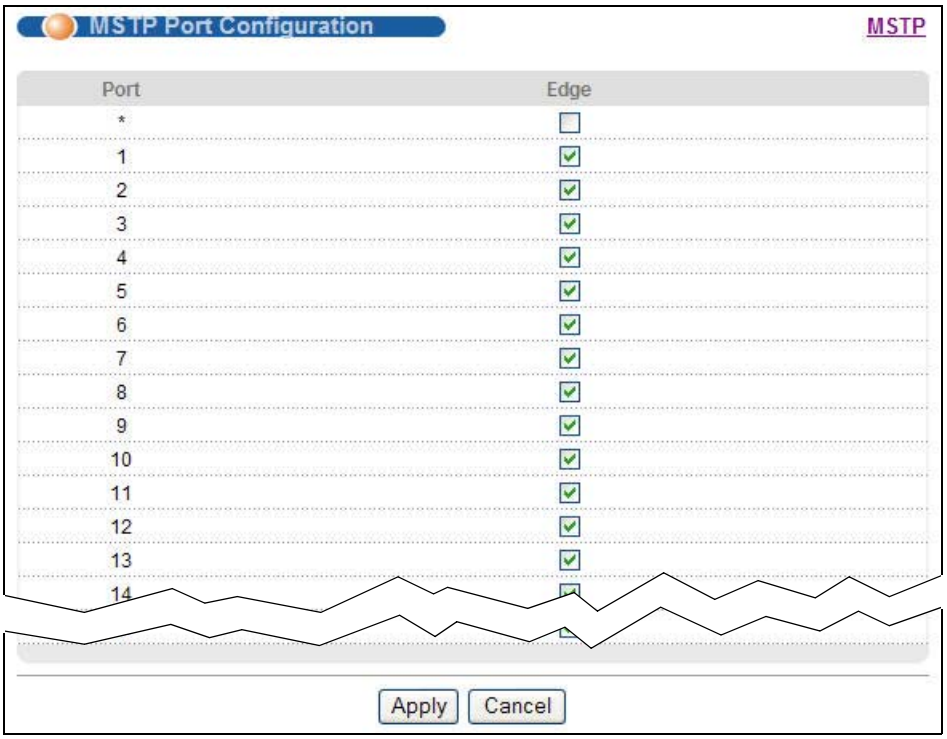
Table 38 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
Enabled VLAN(s)	This field displays which VLAN(s) are mapped to this MST instance.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to add this port to the MST instance.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in the Switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 31 on page 107 for more information.
Add	Click **Add** to save this MST instance to the Switch's run-time memory. The Switch loses this change if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Instance	This field displays the ID of an MST instance.
VLAN	This field displays the VID (or VID ranges) to which the MST instance is mapped.
Active Port	This field display the ports configured to participate in the MST instance.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.8.1 Multiple Spanning Tree Protocol Port Configuration

To configure MSTP ports, click **Port** in the **Advanced Application** > **Spanning Tree Protocol** > **MSTP** screen.

Figure 59 Advanced Application > Spanning Tree Protocol > MSTP > Port



The following table describes the labels in this screen.

Table 39 Advanced Application > Spanning Tree Protocol > MSTP > Port

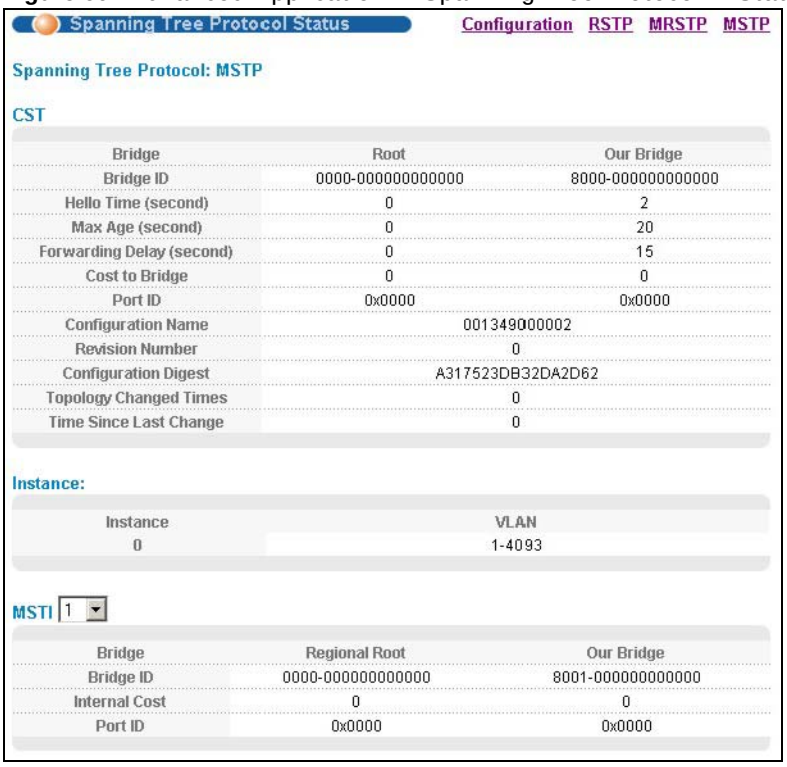
LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

11.9 Multiple Spanning Tree Protocol Status

Click **Advanced Application** > **Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See Section 11.1.5 on page 109 for more information on MSTP.

Note: This screen is only available after you activate MSTP on the Switch.

Figure 60 Advanced Application > Spanning Tree Protocol > Status: MSTP



The following table describes the labels in this screen.

Table 40 Advanced Application > Spanning Tree Protocol > Status: MSTP

LABEL	DESCRIPTION
Configuration	Click **Configuration** to specify which STP mode you want to activate. Click **MSTP** to edit MSTP settings on the Switch.
CST	This section describes the Common Spanning Tree settings.
Bridge	**Root** refers to the base of the spanning tree (the root bridge). **Our Bridge** is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message.
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.

Table 40 Advanced Application > Spanning Tree Protocol > Status: MSTP (continued)

LABEL	DESCRIPTION
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Configuration Name	This field displays the configuration name for this MST region.
Revision Number	This field displays the revision number for this MST region.
Configuration Digest	A configuration digest is generated from the VLAN-MSTI mapping information. This field displays the 16-octet signature that is included in an MSTP BPDU. This field displays the digest when MSTP is activated on the system.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Instance:	These fields display the MSTI to VLAN mapping. In other words, which VLANs run on each spanning tree instance.
Instance	This field displays the MSTI ID.
VLAN	This field displays which VLANs are mapped to an MSTI.
MSTI	Select the MST instance settings you want to view.
Bridge	**Root** refers to the base of the MST instance. **Our Bridge** is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for **Root** and **Our Bridge** if the Switch is the root switch.
Internal Cost	This is the path cost from the root port in this MST instance to the regional root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the MST instance.

12

Bandwidth Control

This chapter shows you how you can cap the maximum bandwidth using the **Bandwidth Control** screen.

12.1 Bandwidth Control Overview

Bandwidth control means defining a maximum allowable bandwidth for incoming and/or out-going traffic flows on a port.

12.1.1 CIR and PIR

The Committed Information Rate (CIR) is the guaranteed bandwidth for the incoming traffic flow on a port. The Peak Information Rate (PIR) is the maximum bandwidth allowed for the incoming traffic flow on a port when there is no network congestion.

The CIR and PIR should be set for all ports that use the same uplink bandwidth. If the CIR is reached, packets are sent at the rate up to the PIR. When network congestion occurs, packets through the ingress port exceeding the CIR will be marked for drop.

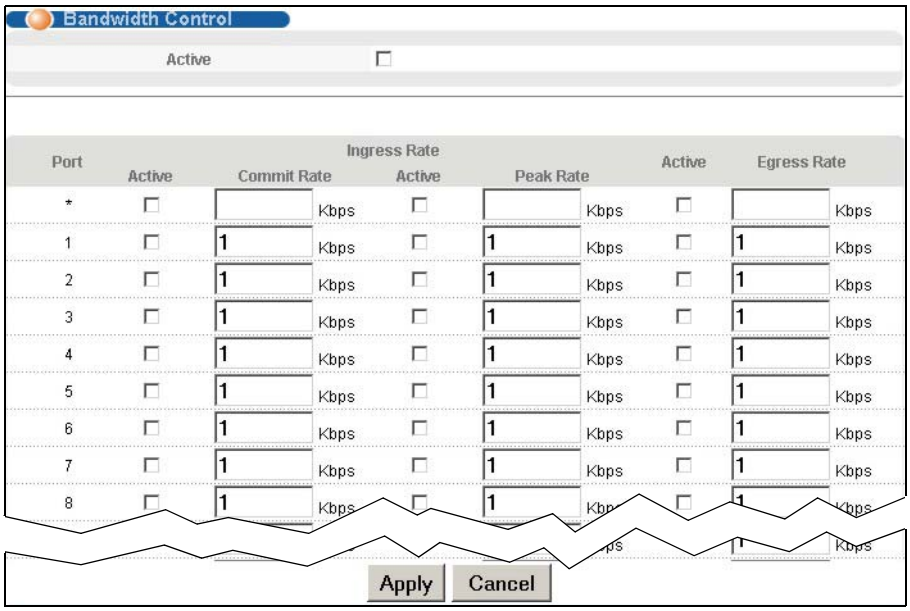
Note: The CIR should be less than the PIR.

Note: The sum of CIRs cannot be greater than or equal to the uplink bandwidth.

12.2 Bandwidth Control Setup

Click **Advanced Application > Bandwidth Control** in the navigation panel to bring up the screen as shown next.

Figure 61 Advanced Application > Bandwidth Control



The following table describes the related labels in this screen.

Table 41 Advanced Application > Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Rate	
Active	Select this check box to activate commit rate limits on this port.
Commit Rate	Specify the guaranteed bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. The commit rate should be less than the peak rate. The sum of commit rates cannot be greater than or equal to the uplink bandwidth.
Active	Select this check box to activate peak rate limits on this port.
Peak Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.
Active	Select this check box to activate egress rate limits on this port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on a port.

Table 41 Advanced Application > Bandwidth Control (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13

Broadcast Storm Control

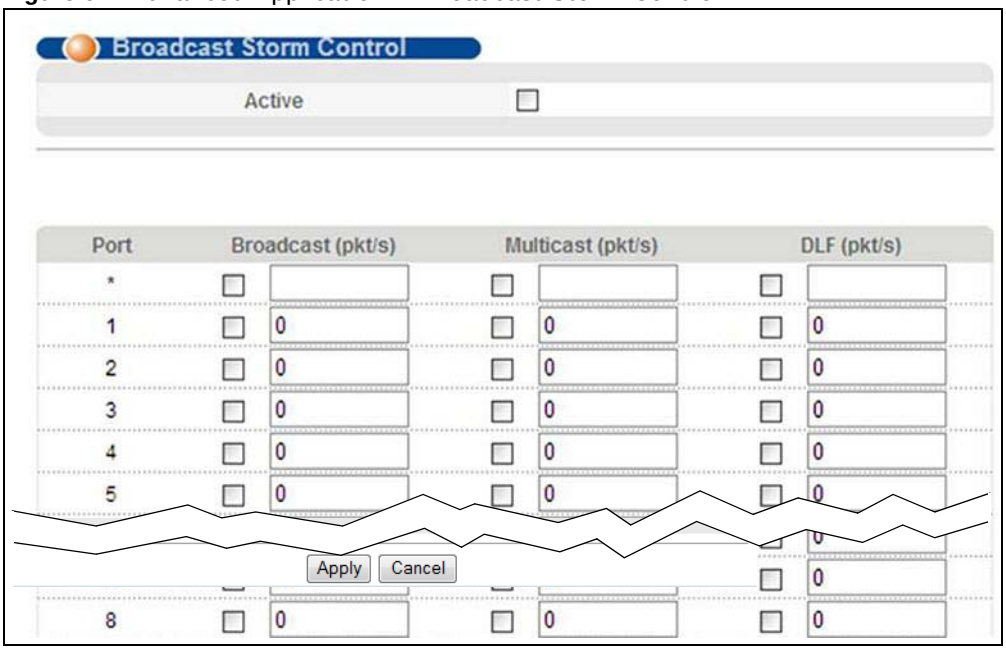
This chapter introduces and shows you how to configure the broadcast storm control feature.

13.1 Broadcast Storm Control Setup

Broadcast storm control limits the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports. When the maximum number of allowable broadcast, multicast and/or DLF packets is reached per second, the subsequent packets are discarded. Enable this feature to reduce broadcast, multicast and/or DLF packets in your network. You can specify limits for each packet type on each port.

Click **Advanced Application** > **Broadcast Storm Control** in the navigation panel to display the screen as shown next.

Figure 62 Advanced Application > Broadcast Storm Control



The following table describes the labels in this screen.

Table 42 Advanced Application > Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable traffic storm control on the Switch. Clear this check box to disable this feature.
Port	This field displays a port number.

Table 42 Advanced Application > Broadcast Storm Control (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second. The allowed range is 0 to 33554431.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second. The allowed range is 0 to 33554431.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second. The allowed range is 0 to 33554431.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14

Mirroring

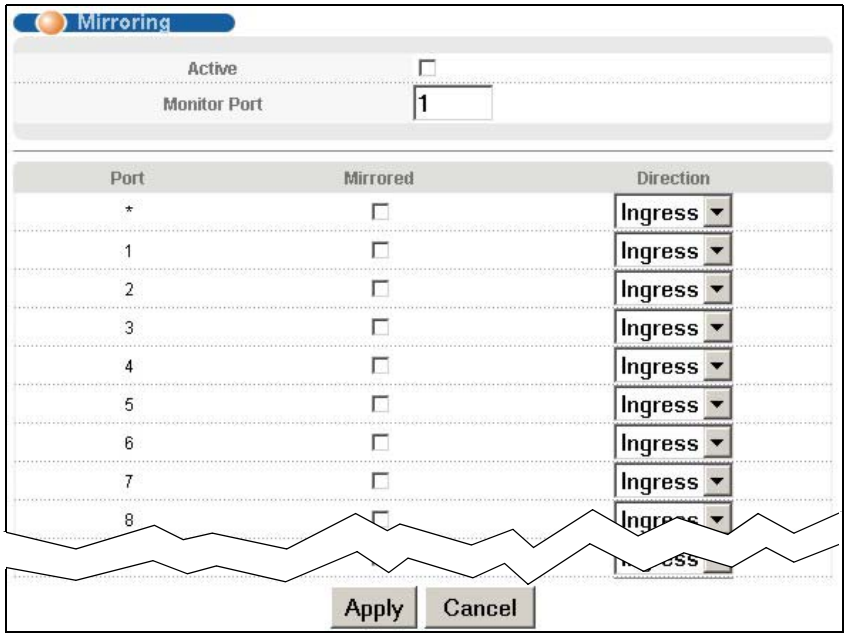
This chapter discusses port mirroring setup screens.

14.1 Port Mirroring Setup

Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

Click **Advanced Application** > **Mirroring** in the navigation panel to display the **Mirroring** screen. Use this screen to select a monitor port and specify the traffic flow to be copied to the monitor port.

Figure 63 Advanced Application > Mirroring



The following table describes the labels in this screen.

Table 43 Advanced Application > Mirroring

LABEL	DESCRIPTION
Active	Select this check box to activate port mirroring on the Switch. Clear this check box to disable the feature.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Type the port number of the monitor port.
Port	This field displays the port number.

Table 43 Advanced Application > Mirroring (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror by selecting from the drop-down list box. Choices are **Egress** (outgoing), **Ingress** (incoming) and **Both**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15

Link Aggregation

This chapter shows you how to logically aggregate physical links to form one logical, higher-bandwidth link.

15.1 Link Aggregation Overview

Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link.

However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

The beginning port of each trunk group must be physically connected to form a trunk group.

The Switch supports both static and dynamic link aggregation.

Note: In a properly planned network, it is recommended to implement static link aggregation only. This ensures increased network stability and control over the trunk groups on your Switch.

See Section 15.6 on page 138 for a static port trunking example.

15.2 Dynamic Link Aggregation

The Switch adheres to the IEEE 802.3ad standard for static and dynamic (LACP) port trunking.

The Switch supports the link aggregation IEEE802.3ad standard. This standard describes the Link Aggregation Control Protocol (LACP), which is a protocol that dynamically creates and manages trunk groups.

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an operational port fails, then one of the “standby” ports become operational without user intervention. Please note that:

- You must connect all ports point-to-point to the same Ethernet switch and configure the ports for LACP trunking.
- LACP only works on full-duplex links.
- All ports in the same trunk group must have the same media type, speed, duplex mode and flow control settings.

Configure trunk groups or LACP before you connect the Ethernet switch to avoid causing network topology loops.

15.2.1 Link Aggregation ID

LACP aggregation ID consists of the following information[1]:

Table 44 Link Aggregation ID: Local Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

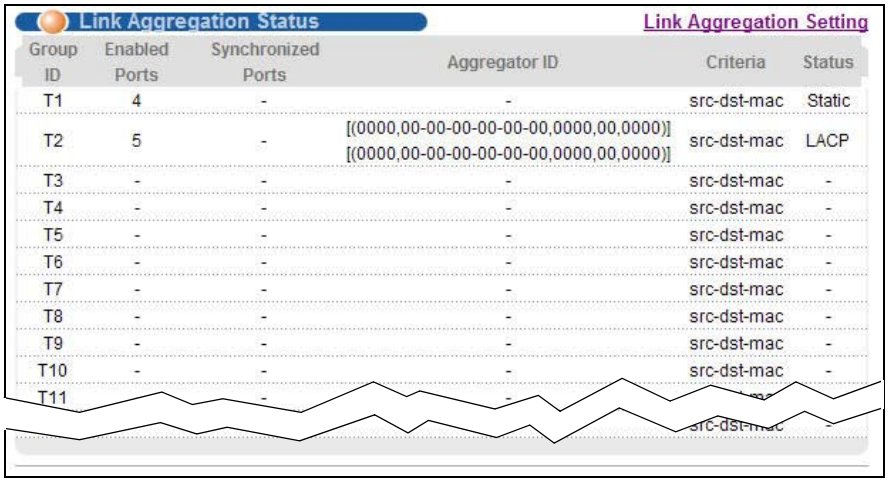
Table 45 Link Aggregation ID: Peer Switch

SYSTEM PRIORITY	MAC ADDRESS	KEY	PORT PRIORITY	PORT NUMBER
0000	00-00-00-00-00-00	0000	00	0000

15.3 Link Aggregation Status

Click **Advanced Application** > **Link Aggregation** in the navigation panel. The **Link Aggregation Status** screen displays by default. See Section 15.1 on page 132 for more information.

Figure 64 Advanced Application > Link Aggregation Status


Link Aggregation Status
Link Aggregation Setting
Group ID
Enabled Ports
Synchronized Ports
Aggregator ID
Criteria
Status
T1 4 - - src-dst-mac Static
T2 5 - [(0000,00-00-00-00-00-00,0000,00,0000)] [(0000,00-00-00-00-00-00,0000,00,0000)] src-dst-mac LACP
T3 - - - src-dst-mac -
T4 - - - src-dst-mac -
T5 - - - src-dst-mac -
T6 - - - src-dst-mac -
T7 - - - src-dst-mac -
T8 - - - src-dst-mac -
T9 - - - src-dst-mac -
T10 - - - src-dst-mac -
T11 - - -

The following table describes the labels in this screen.

Table 46 Advanced Application > Link Aggregation Status

LABEL	DESCRIPTION
Group ID	This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Port	These are the ports you have configured in the **Link Aggregation** screen to be in the trunk group. The port number(s) displays only when this trunk group is activated and there is a port belonging to this group.

1. Port Priority and Port Number are 0 as it is the aggregator ID for the trunk group, not the individual port.

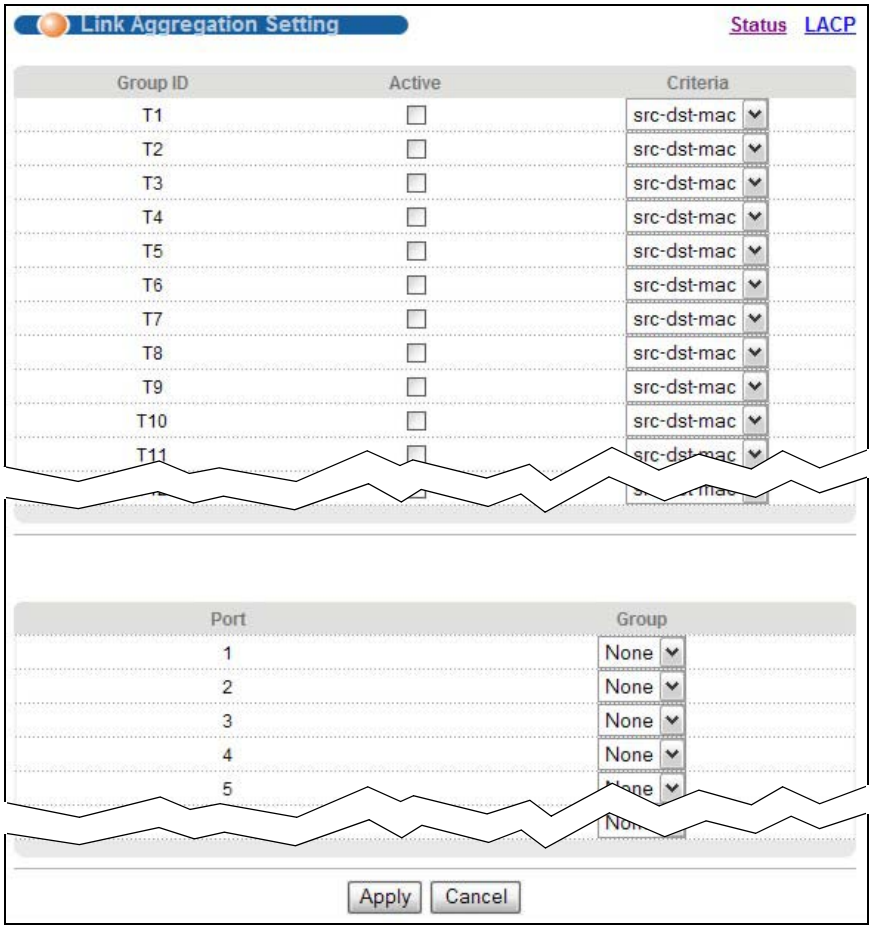
Table 46 Advanced Application > Link Aggregation Status (continued)

LABEL	DESCRIPTION
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Aggregator ID	Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to Section 15.2.1 on page 133 for more information on this field. The ID displays only when there is a port belonging to this trunk group and LACP is also enabled for this group.
Criteria	This shows the outgoing traffic distribution algorithm used in this trunk group. Packets from the same source and/or to the same destination are sent over the same link within the trunk. **src-mac** means the Switch distributes traffic based on the packet's source MAC address. **dst-mac** means the Switch distributes traffic based on the packet's destination MAC address. **src-dst-mac** means the Switch distributes traffic based on a combination of the packet's source and destination MAC addresses. **src-ip** means the Switch distributes traffic based on the packet's source IP address. **dst-ip** means the Switch distributes traffic based on the packet's destination IP address. **src-dst-ip** means the Switch distributes traffic based on a combination of the packet's source and destination IP addresses.
Status	This field displays how these ports were added to the trunk group. It displays: • **Static** - if the ports are configured as static members of a trunk group. • **LACP** - if the ports are configured to join a trunk group via LACP.

15.4 Link Aggregation Setting

Click **Advanced Application** > **Link Aggregation > Link Aggregation Setting** to display the screen shown next. See Section 15.1 on page 132 for more information on link aggregation.

Figure 65 Advanced Application > Link Aggregation > Link Aggregation Setting



The following table describes the labels in this screen.

Table 47 Advanced Application > Link Aggregation > Link Aggregation Setting

LABEL	DESCRIPTION
Link Aggregation Setting	This is the only screen you need to configure to enable static link aggregation.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
Active	Select this option to activate a trunk group.

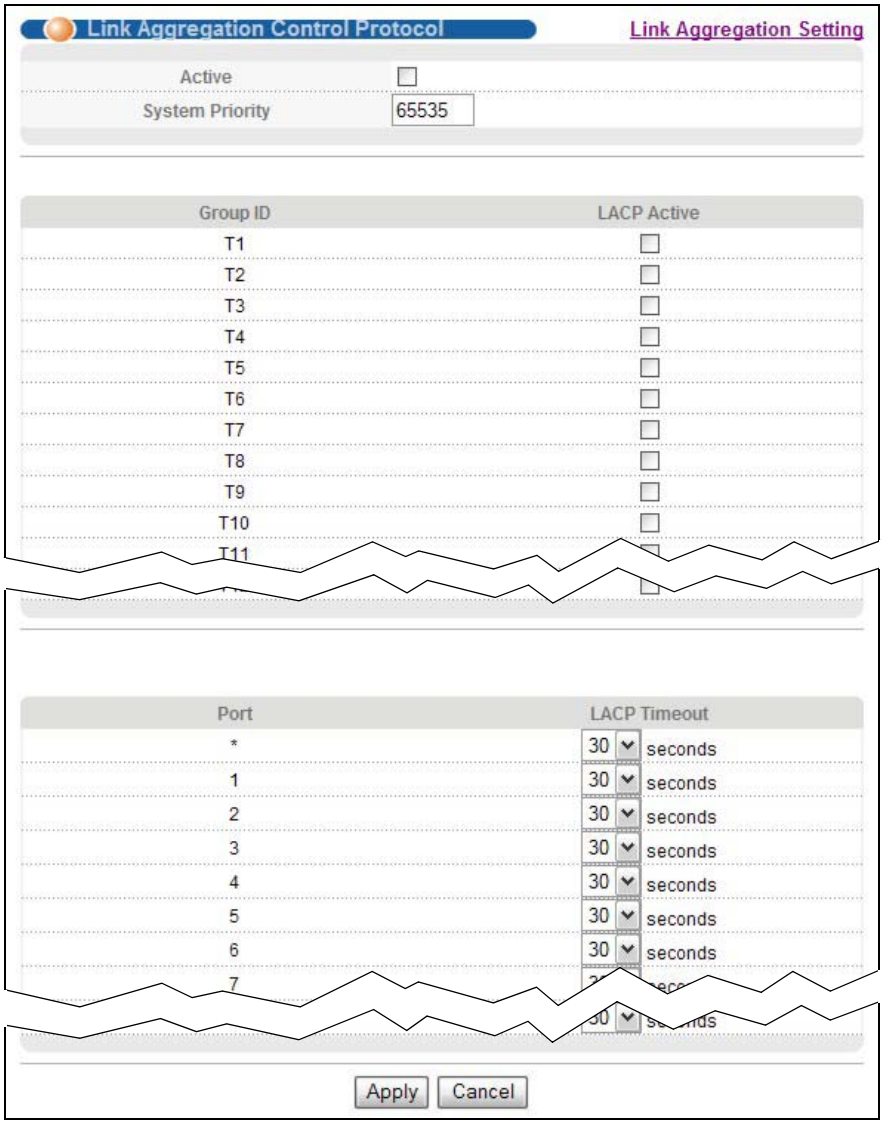
Table 47 Advanced Application > Link Aggregation > Link Aggregation Setting (continued)

LABEL	DESCRIPTION
Criteria	Select the outgoing traffic distribution type. Packets from the same source and/or to the same destination are sent over the same link within the trunk. By default, the Switch uses the **src-dst-mac** distribution type. If the Switch is behind a router, the packet's destination or source MAC address will be changed. In this case, set the Switch to distribute traffic based on its IP address to make sure port trunking can work properly. Select **src-mac** to distribute traffic based on the packet's source MAC address. Select **dst-mac** to distribute traffic based on the packet's destination MAC address. Select **src-dst-mac** to distribute traffic based on a combination of the packet's source and destination MAC addresses. Select **src-ip** to distribute traffic based on the packet's source IP address. Select **dst-ip** to distribute traffic based on the packet's destination IP address. Select **src-dst-ip** to distribute traffic based on a combination of the packet's source and destination IP addresses.
Port	This field displays the port number.
Group	Select the trunk group to which a port belongs. Note: When you enable the port security feature on the Switch and configure port security settings for a port, you cannot include the port in an active trunk group.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.5 Link Aggregation Control Protocol

Click in the **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting** > **LACP** to display the screen shown next. See Section 15.2 on page 132 for more information on dynamic link aggregation.

Figure 66 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP



The following table describes the labels in this screen.

Table 48 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

LABEL	DESCRIPTION
Link Aggregation Control Protocol	Note: Do not configure this screen unless you want to enable dynamic link aggregation.
Active	Select this checkbox to enable Link Aggregation Control Protocol (LACP).

Table 48 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (continued)

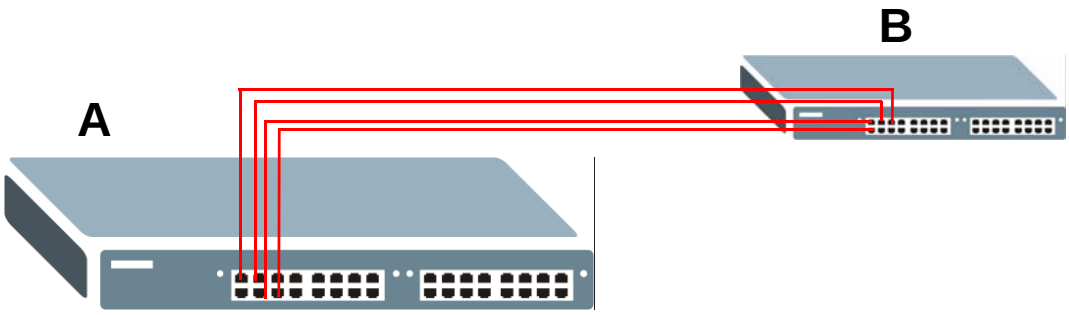
LABEL	DESCRIPTION
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “server”. The LACP “server” controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP Active	Select this option to enable LACP for a trunk.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds.
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

15.6 Static Trunking Example

This example shows you how to create a static port trunk group for ports 2-5.

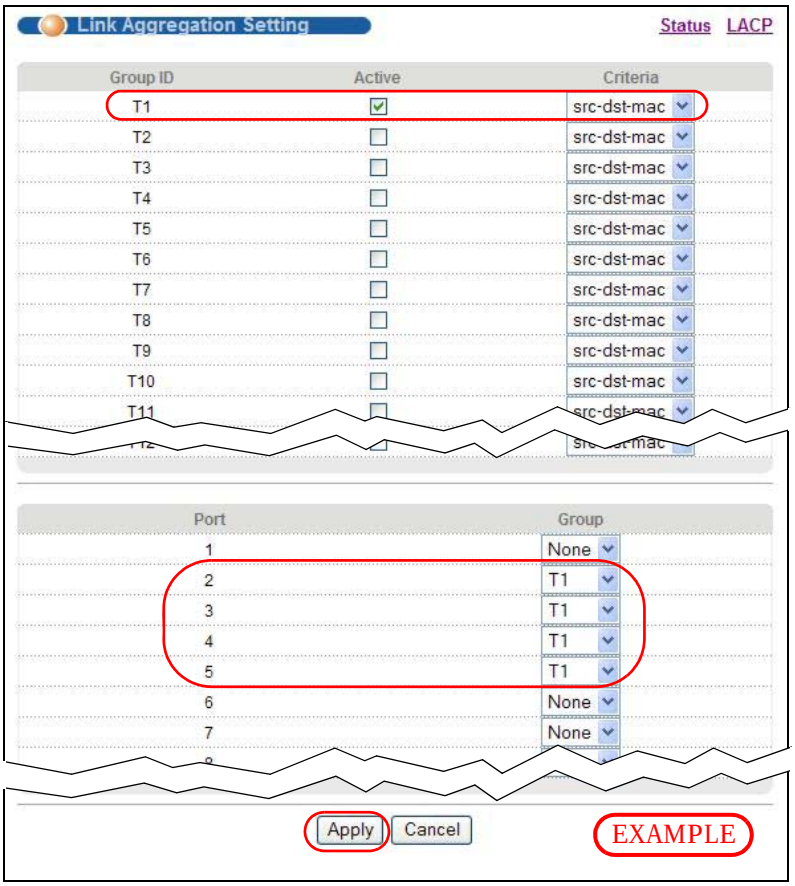
1 **Make your physical connections** - make sure that the ports that you want to belong to the trunk group are connected to the same destination. The following figure shows ports 2-5 on switch **A** connected to switch **B**.

Figure 67 Trunking Example - Physical Connections



2 **Configure static trunking** - Click **Advanced Application** > **Link Aggregation** > **Link Aggregation Setting**. In this screen activate trunk group **T1**, select the traffic distribution algorithm used by this group and select the ports that should belong to this group as shown in the figure below. Click **Apply** when you are done.

Figure 68 Trunking Example - Configuration Screen



Your trunk group 1 (**T1**) configuration is now complete.

16

Port Authentication

This chapter describes the IEEE 802.1x and MAC authentication methods.

16.1 Port Authentication Overview

Port authentication is a way to validate access to ports on the Switch to clients based on an external server (authentication server). The Switch supports the following methods for port authentication:

- **IEEE 802.1x**[2] - An authentication server validates access to a port based on a username and password provided by the user.
- **MAC** - An authentication server validates access to a port based on the MAC address and password of the client.

Both types of authentication use the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. See Section 23.1.2 on page 188 for more information on configuring your RADIUS server settings.

If you enable IEEE 802.1x authentication and MAC authentication on the same port, the Switch performs IEEE 802.1x authentication first. If a user fails to authenticate via the IEEE 802.1x method, then access to the port is denied.

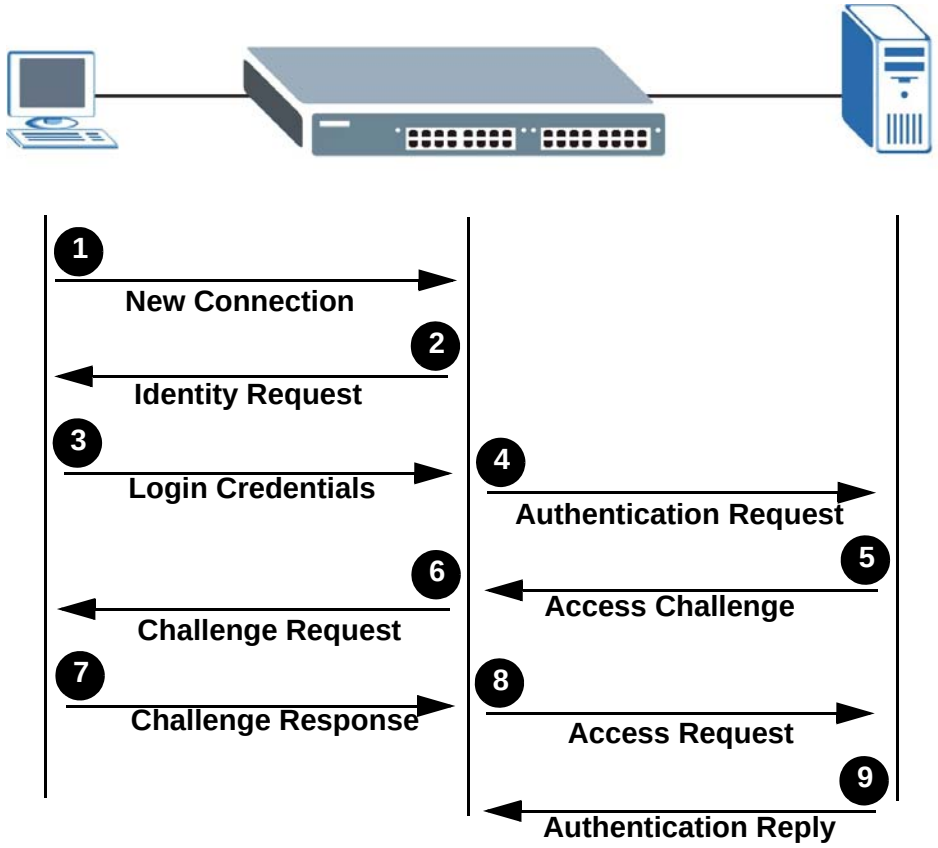
16.1.1 IEEE 802.1x Authentication

The following figure illustrates how a client connecting to an IEEE 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password after the client responds to its identity request. When the client

2. At the time of writing, IEEE 802.1x is not supported by all operating systems. See your operating system documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

provides the login credentials, the Switch sends an authentication request to a RADIUS server. The RADIUS server validates whether this client is allowed access to the port.

Figure 69 IEEE 802.1x Authentication Process

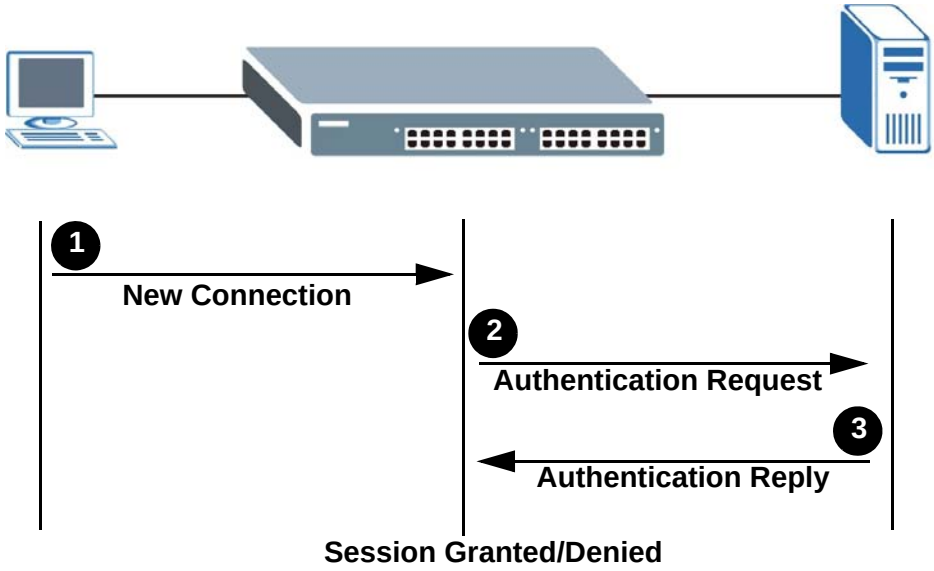


16.1.2 MAC Authentication

MAC authentication works in a very similar way to IEEE 802.1x authentication. The main difference is that the Switch does not prompt the client for login credentials. The login credentials are based

on the source MAC address of the client connecting to a port on the Switch along with a password configured specifically for MAC authentication on the Switch.

Figure 70 MAC Authentication Process



16.2 Port Authentication Configuration

To enable port authentication, first activate the port authentication method(s) you want to use (both on the Switch and the port(s)), then configure the RADIUS server settings in the **AAA > Radius Server Setup** screen.

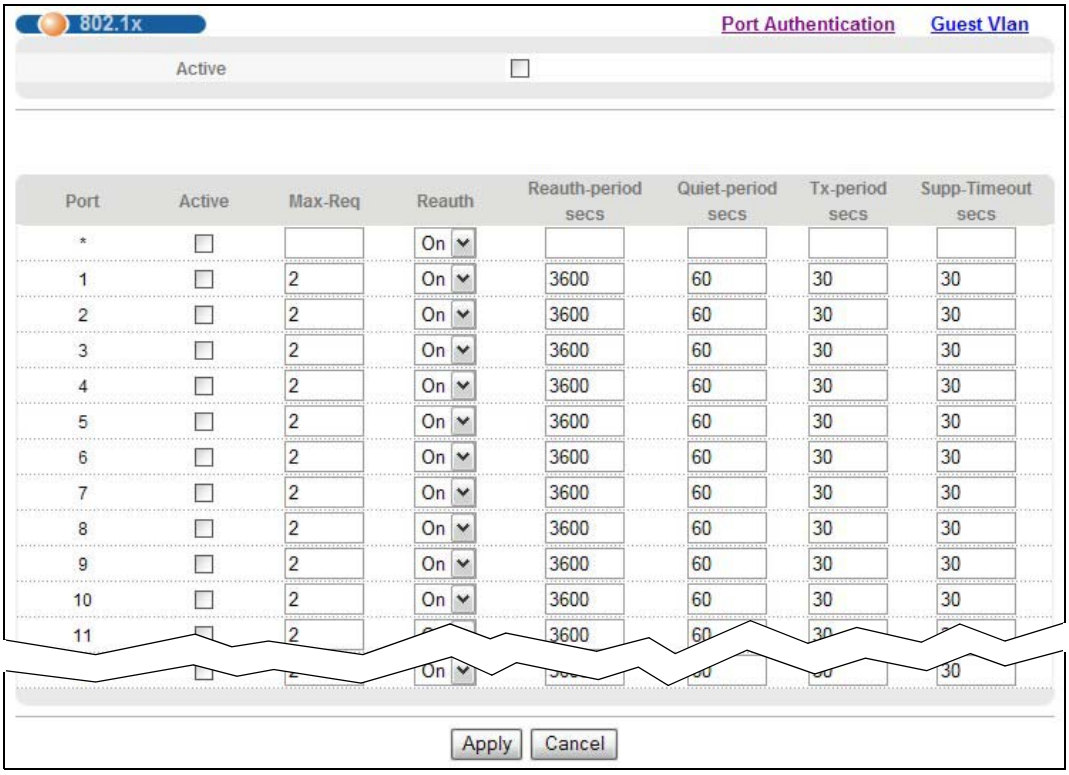
To activate a port authentication method, click **Advanced Application** > **Port Authentication** in the navigation panel. Select a port authentication method in the screen that appears.

Figure 71 Advanced Application > Port Authentication

16.2.1 Activate IEEE 802.1x Security

Use this screen to activate IEEE 802.1x security. In the **Port Authentication** screen click **802.1x** to display the configuration screen as shown.

Figure 72 Advanced Application > Port Authentication > 802.1x



The following table describes the labels in this screen.

Table 49 Advanced Application > Port Authentication > 802.1x

LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the Switch. Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the Switch before configuring it on each port.
Max-Req	Specify the number of times the Switch tries to authenticate client(s) before sending unresponsive ports to the Guest VLAN. This is set to 2 by default. That is, the Switch attempts to authenticate a client twice. If the client does not respond to the first authentication request, the Switch tries again. If the client still does not respond to the second request, the Switch sends the client to the Guest VLAN. The client needs to send a new request to be authenticated by the Switch again.

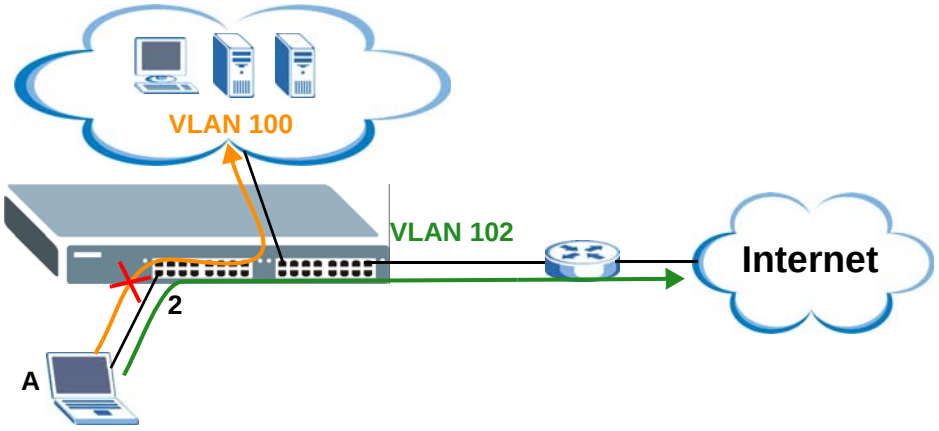
Table 49 Advanced Application > Port Authentication > 802.1x (continued)

LABEL	DESCRIPTION
Reauth	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauth-period	Specify the length of time required to pass before a client has to re-enter his or her username and password to stay connected to the port.
Quiet-period	Specify the number of seconds the port remains in the HELD state and rejects further authentication requests from the connected client after a failed authentication exchange.
Tx-period	Specify the number of seconds the Switch waits for client's response before re-sending an identity request to the client.
Supp-Timeout	Specify the number of seconds the Switch waits for client's response to a challenge request before sending another request.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16.2.2 Guest VLAN

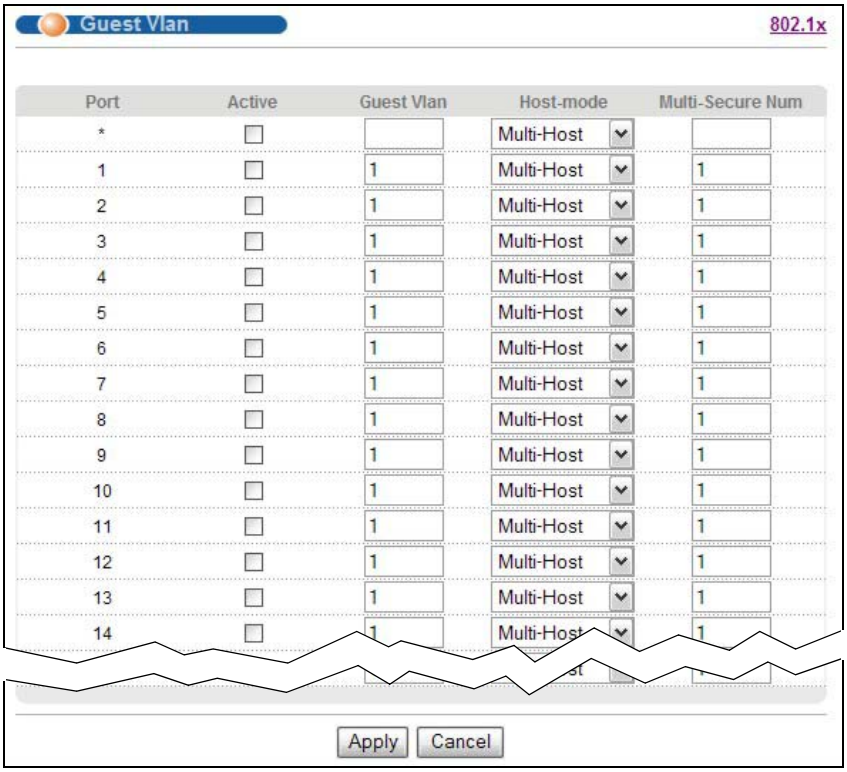
When 802.1x port authentication is enabled on the Switch and its ports, clients that do not have the correct credentials are blocked from using the port(s). You can configure your Switch to have one VLAN that acts as a guest VLAN. If you enable the guest VLAN (**102** in the example) on a port (**2** in the example), the user (**A** in the example) that is not IEEE 802.1x capable or fails to enter the correct username and password can still access the port, but traffic from the user is forwarded to the guest VLAN. That is, unauthenticated users can have access to limited network resources in the same guest VLAN, such as the Internet. The rights granted to the Guest VLAN depends on how the network administrator configures switches or routers with the guest network feature.

Figure 73 Guest VLAN Example



Use this screen to enable and assign a guest VLAN to a port. In the **Port Authentication > 802.1x** screen click **Guest Vlan** to display the configuration screen as shown.

Figure 74 Advanced Application > Port Authentication > 802.1x > Guest VLAN



The following table describes the labels in this screen.

Table 50 Advanced Application > Port Authentication > 802.1x > Guest VLAN

LABEL	DESCRIPTION
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to enable the guest VLAN feature on this port. Clients that fail authentication are placed in the guest VLAN and can receive limited services.
Guest Vlan	A guest VLAN is a pre-configured VLAN on the Switch that allows non-authenticated users to access limited network resources through the Switch. You must also enable IEEE 802.1x authentication on the Switch and the associated ports. Enter the number that identifies the guest VLAN. Make sure this is a VLAN recognized in your network.

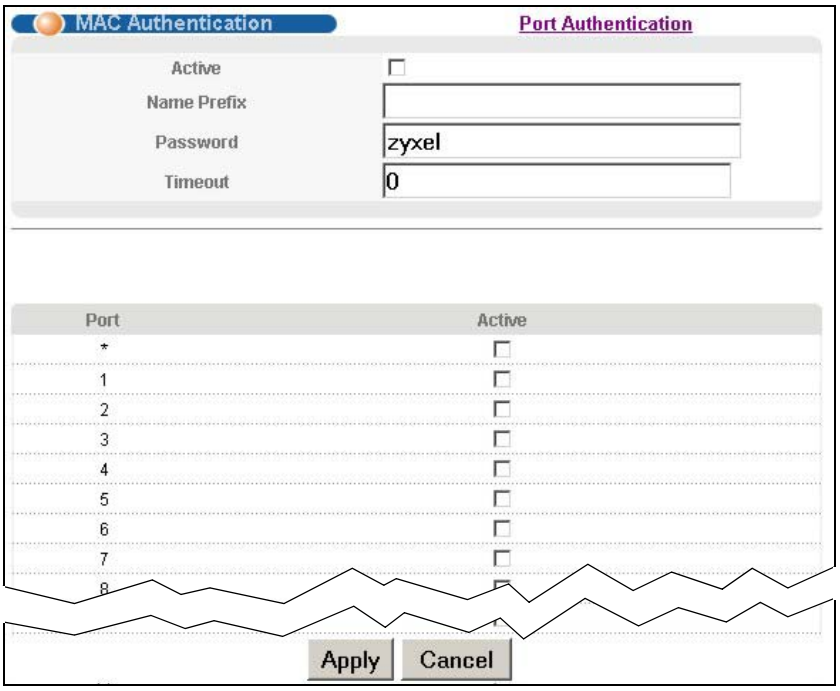
Table 50 Advanced Application > Port Authentication > 802.1x > Guest VLAN (continued)

LABEL	DESCRIPTION
Host-mode	Specify how the Switch authenticates users when more than one user connect to the port (using a hub). Select **Multi-Host** to authenticate only the first user that connects to this port. If the first user enters the correct credential, any other users are allowed to access the port without authentication. If the first user fails to enter the correct credential, they are all put in the guest VLAN. Once the first user who did authentication logs out or disconnects from the port, rest of the users are blocked until a user does the authentication process again. Select **Multi-Secure** to authenticate each user that connects to this port.
Multi-Secure Num	If you set **Host-mode** to **Multi-Secure**, specify the maximum number of users (between 1 and 24) that the Switch will authenticate on this port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

16.2.3 Activate MAC Authentication

Use this screen to activate MAC authentication. In the **Port Authentication** screen click **MAC Authentication** to display the configuration screen as shown.

Figure 75 Advanced Application > Port Authentication > MAC Authentication



The following table describes the labels in this screen.

Table 51 Advanced Application > Port Authentication > MAC Authentication

LABEL	DESCRIPTION
Active	Select this check box to permit MAC authentication on the Switch. Note: You must first enable MAC authentication on the Switch before configuring it on each port.
Name Prefix	Type the prefix that is appended to all MAC addresses sent to the RADIUS server for authentication. You can enter up to 32 printable ASCII characters. If you leave this field blank, then only the MAC address of the client is forwarded to the RADIUS server.
Password	Type the password the Switch sends along with the MAC address of a client for authentication with the RADIUS server. You can enter up to 32 printable ASCII characters.
Timeout	Specify the amount of time before the Switch allows a client MAC address that fails authentication to try and authenticate again. Maximum time is 3000 seconds. When a client fails MAC authentication, its MAC address is learned by the MAC address table with a status of denied. The timeout period you specify here is the time the MAC address entry stays in the MAC address table until it is cleared. If you specify 0 for the timeout value, then this entry will not be deleted from the MAC address table. Note: If the **Aging Time** in the **Switch Setup** screen is set to a lower value, then it supersedes this setting. See Section 6.5 on page 74.
Port	This field displays a port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to permit MAC authentication on this port. You must first allow MAC authentication on the Switch before configuring it on each port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17

Port Security

This chapter shows you how to set up port security.

17.1 About Port Security

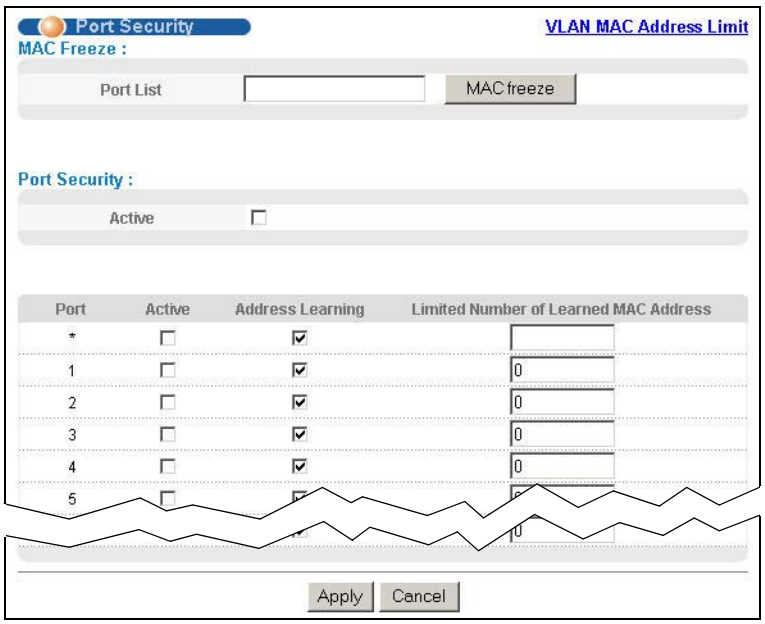
Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch. The Switch can learn up to 32K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 32K.

For maximum port security, enable this feature, disable MAC address learning and configure static MAC address(es) for a port. It is not recommended you disable port security together with MAC address learning as this will result in many broadcasts. By default, MAC address learning is still enabled even though the port security is not activated.

17.2 Port Security Setup

Click **Advanced Application** > **Port Security** in the navigation panel to display the screen as shown.

Figure 76 Advanced Application > Port Security



The following table describes the labels in this screen.

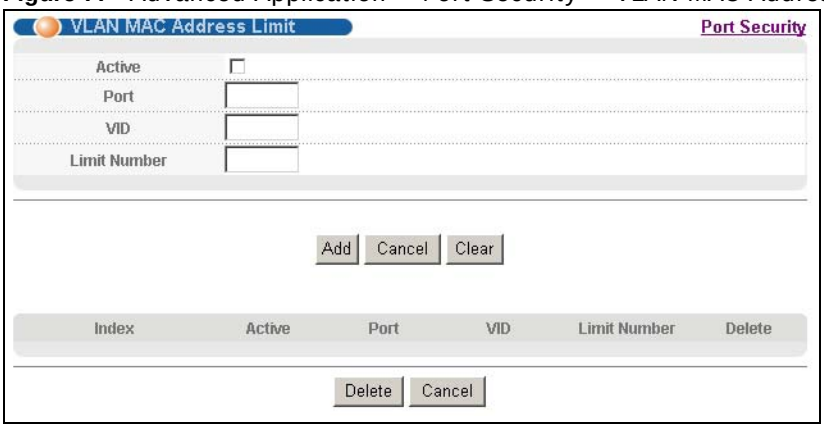
Table 52 Advanced Application > Port Security

LABEL	DESCRIPTION
Port List	Enter the number of the port(s) (separated by a comma) on which you want to enable port security and disable MAC address learning. After you click **MAC freeze**, all previously learned MAC addresses on the specified port(s) will become static MAC addresses and display in the **Static MAC Forwarding** screen.
MAC freeze	Click **MAC freeze** to have the Switch automatically select the **Active** check boxes and clear the **Address Learning** check boxes only for the ports specified in the **Port list**.
Active	Select this option to enable port security on the Switch.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some of the settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the port security feature on this port. The Switch forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped. Clear this check box to disable the port security feature. The Switch forwards all packets on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device must wait until one of the five learned MAC addresses ages out. MAC address aging out time can be set in the **Switch Setup** screen. The valid range is from “0” to “16384”. “0” means this feature is disabled.
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

17.3 VLAN MAC Address Limit

Use this screen to set the MAC address learning limit on per-port and per-VLAN basis. Click **VLAN MAC Address Limit** in the **Advanced Application > Port Security** screen to display the screen as shown.

Figure 77 Advanced Application > Port Security > VLAN MAC Address Limit



The following table describes the labels in this screen.

Table 53 Advanced Application > Port Security > VLAN MAC Address Limit

LABEL	DESCRIPTION
Active	Select this option to activate this rule.
Port	Enter the number of the port to which this rule is applied.
VID	Enter the VLAN identification number.
Limit Number	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port in a specified VLAN. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the **Switch Setup** screen. The valid range is from "0" to "16384". "0" means this feature is disabled.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays **Yes** when the rule is activated and **No** when is it deactivated.
Port	This field displays the number of the port to which this rule is applied.
VID	This is the VLAN ID number to which the port belongs.
Limit Number	This is the maximum number of MAC addresses which a port can learn in a VLAN.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected checkbox(es) in the **Delete** column.

18

Classifier

This chapter introduces and shows you how to configure the packet classifier on the Switch.

18.1 About the Classifier and QoS

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming port number. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

Configure QoS on the Switch to group and prioritize application traffic and fine-tune network performance. Setting up QoS involves two separate steps:

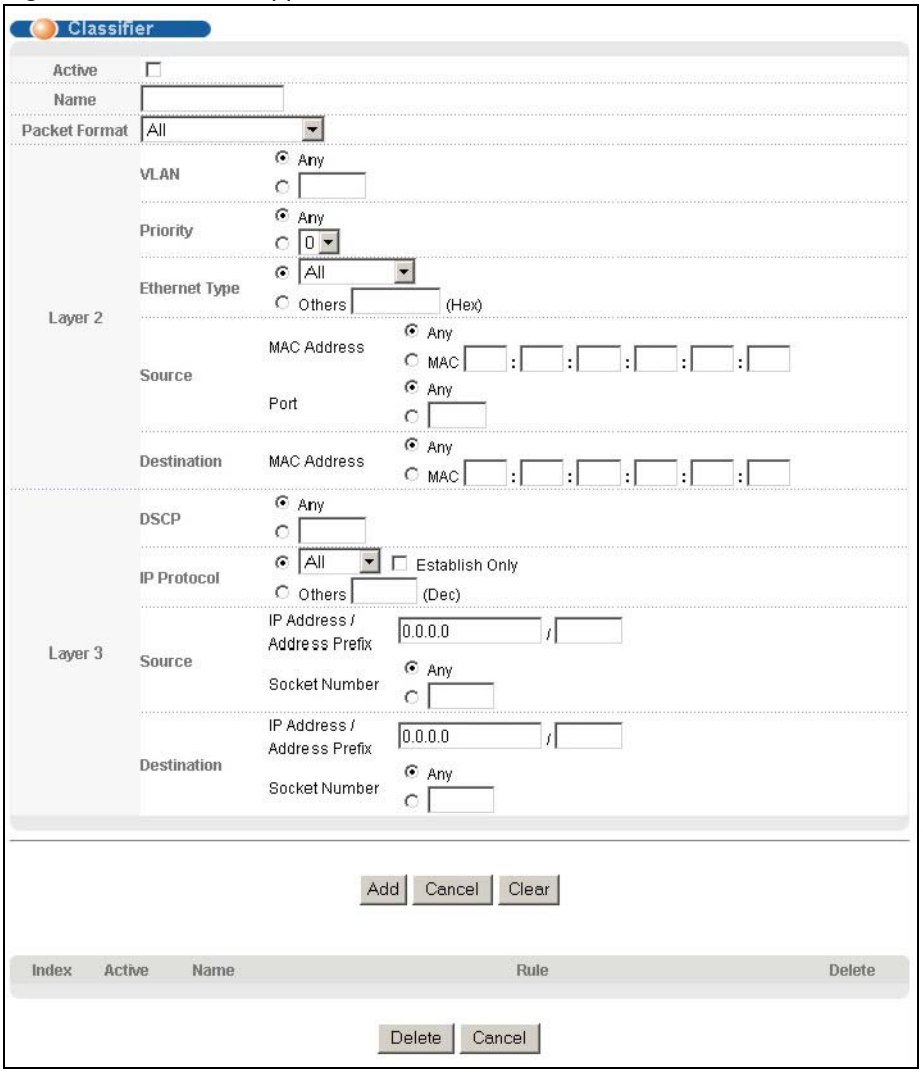
1. Configure classifiers to sort traffic into different flows.
2. Configure policy rules to define actions to be performed for a classified traffic flow (refer to Chapter 19 on page 157 to configure policy rules).

18.2 Configuring the Classifier

Use the **Classifier** screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules. To configure policy rules, refer to Chapter 19 on page 157.

Click **Advanced Application > Classifier** in the navigation panel to display the configuration screen as shown.

Figure 78 Advanced Application > Classifier



The following table describes the labels in this screen.

Table 54 Advanced Application > Classifier

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes.
Packet Format	Specify the format of the packet. Choices are **All**, **802.3 tagged**, **802.3 untagged**, **Ethernet II tagged** and **Ethernet II untagged**. A value of **802.3** indicates that the packets are formatted according to the IEEE 802.3 standards. A value of **Ethernet II** indicates that the packets are formatted according to RFC 894, Ethernet II encapsulation.
Layer 2 Specify the fields below to configure a layer-2 classifier.	

Table 54 Advanced Application > Classifier (continued)

LABEL	DESCRIPTION
VLAN	Select **Any** to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.
Priority	Select **Any** to classify traffic from any priority level or select the second option and specify a priority level in the field provided.
Ethernet Type	Select an Ethernet type or select **Other** and enter the Ethernet type number in hexadecimal value. Refer to Table 56 on page 154 for information.
Source	
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a source, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Port	Type the port number to which the rule should be applied. You may choose one port only or all ports (**Any**).
Destination	
MAC Address	Select **Any** to apply the rule to all MAC addresses. To specify a destination, select the second choice and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Layer 3 Specify the fields below to configure a layer-3 classifier.	
DSCP	Select **Any** to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
IP Protocol	Select an IP protocol type or select **Other** and enter the protocol number in decimal value. Refer to Table 57 on page 155 for more information. You may select **Establish Only** for **TCP** protocol type. This means that the Switch will pick out the packets that are sent to establish TCP connections.
Source	
IP Address/ Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You must select either **UDP** or **TCP** in the **IP Protocol** field before you configure the socket numbers. Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Destination	
IP Address/ Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Socket Number	Note: You must select either **UDP** or **TCP** in the **IP Protocol** field before you configure the socket numbers. Select **Any** to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.

Table 54 Advanced Application > Classifier (continued)

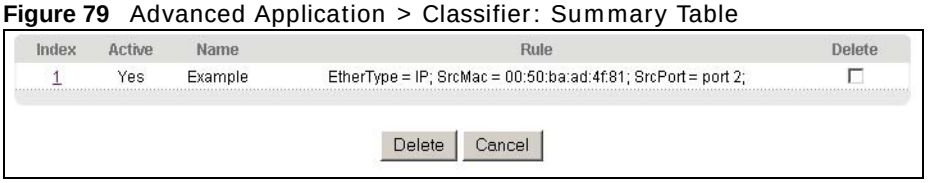
LABEL	DESCRIPTION
Add	Click **Add** to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to set the above fields back to the factory defaults.

18.3 Viewing and Editing Classifier Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Classifier** screen. To change the settings of a rule, click a number in the **Index** field.

Note: When two rules conflict with each other, a higher layer rule has priority over a lower layer rule.

Figure 79 Advanced Application > Classifier: Summary Table



The following table describes the labels in this screen.

Table 55 Classifier: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays **Yes** when the rule is activated and **No** when it is deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purposes only.
Rule	This field displays a summary of the classifier rule's settings.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

The following table shows some other common Ethernet types and the corresponding protocol number.

Table 56 Common Ethernet Types and Protocol Number

ETHERNET TYPE	PROTOCOL NUMBER
IP ETHII	0800
X.75 Internet	0801
NBS Internet	0802
ECMA Internet	0803
Chaosnet	0804
X.25 Level 3	0805
XNS Compat	0807

Table 56 Common Ethernet Types and Protocol Number

ETHERNET TYPE	PROTOCOL NUMBER
Banyan Systems	0BAD
BBN Simnet	5208
IBM SNA	80D5
AppleTalk AARP	80F3

Some of the most common IP ports are:

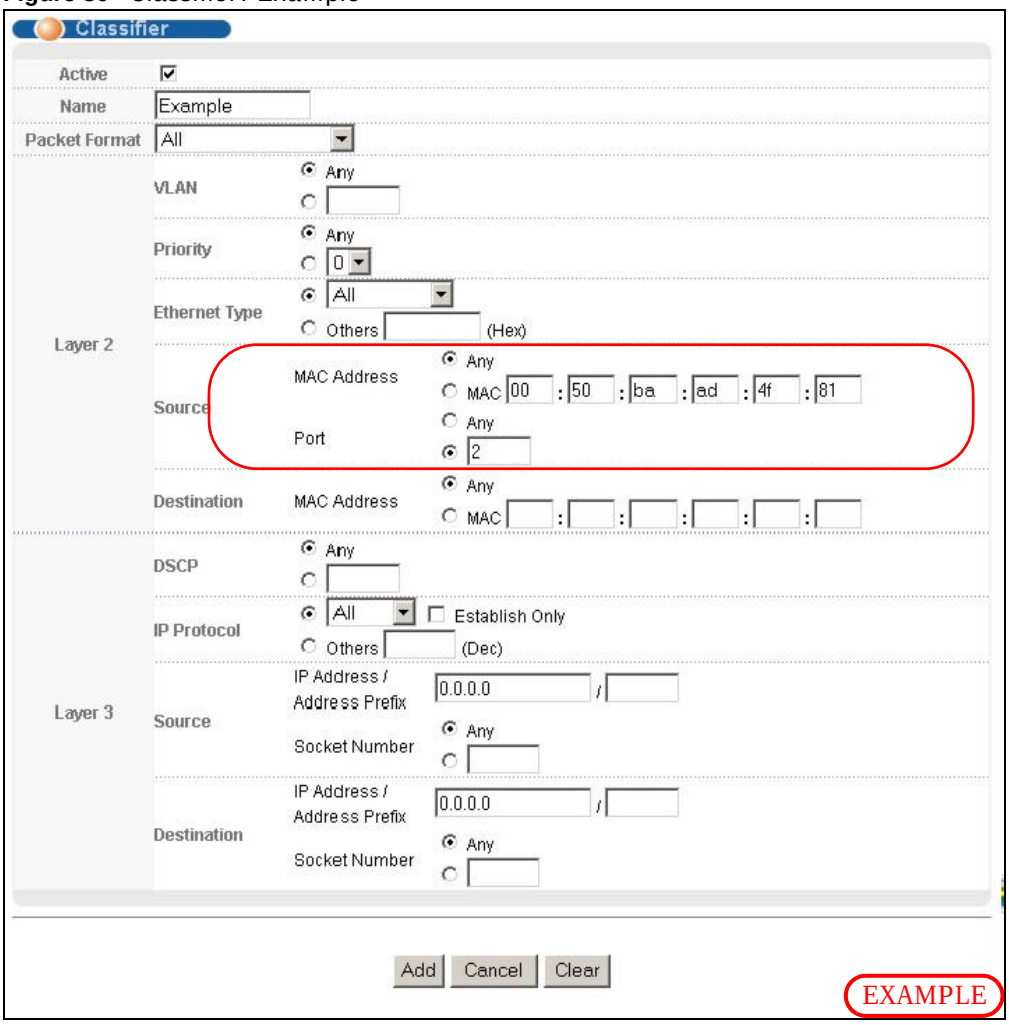
Table 57 Common IP Ports

PORT NUMBER	PORT NAME
21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3

18.4 Classifier Example

The following screen shows an example of configuring a classifier that identifies all traffic from MAC address 00:50:ba:ad:4f:81 on port 2.

Figure 80 Classifier: Example



After you have configured a classifier, you can configure a policy to define action(s) on the classified traffic flow. See Chapter 19 on page 157 for information on configuring a policy rule.

19

Policy Rule

This chapter shows you how to configure policy rules.

19.1 Policy Rules Overview

A classifier distinguishes traffic into flows based on the configured criteria (refer to Chapter 18 on page 151 for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

19.1.1 DiffServ

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

19.1.2 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)

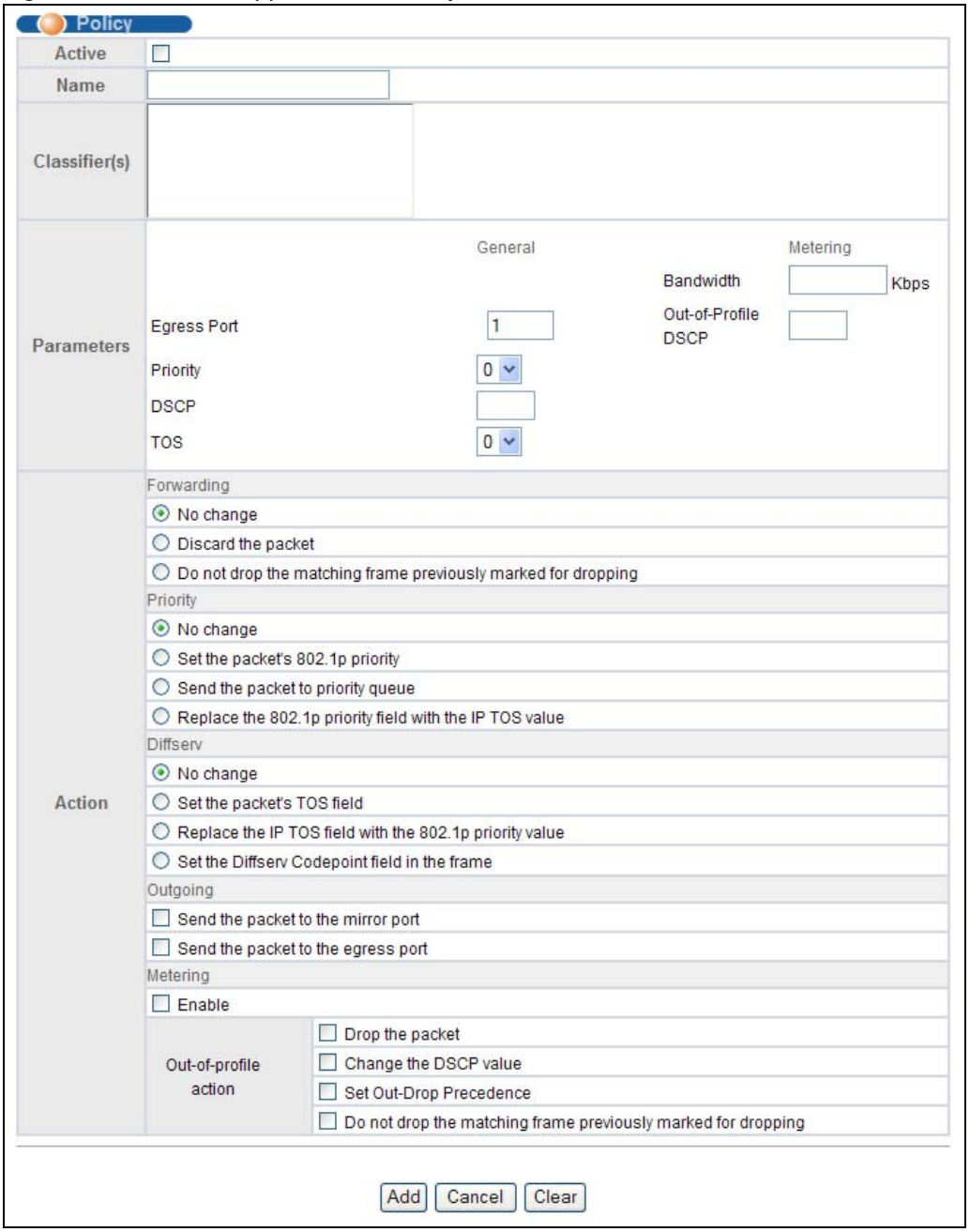
The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

19.2 Configuring Policy Rules

You must first configure a classifier in the **Classifier** screen. Refer to Section 18.2 on page 151 for more information.

Click **Advanced Applications > Policy Rule** in the navigation panel to display the screen as shown.

Figure 81 Advanced Application > Policy Rule



The following table describes the labels in this screen.

Table 58 Advanced Application > Policy Rule

LABEL	DESCRIPTION
Active	Select this option to enable the policy.
Name	Enter a descriptive name for identification purposes.

Table 58 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Classifier(s)	This field displays the active classifier(s) you configure in the **Classifier** screen. Select the classifier(s) to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
Parameters Set the fields below for this policy. You only have to set the field(s) that is related to the action(s) you configure in the **Action** field.	
General	
Egress Port	Type the number of an outgoing port.
Priority	Specify a priority level.
DSCP	Specify a DSCP (DiffServ Code Point) number between 0 and 63.
TOS	Specify the type of service (TOS) priority level.
Metering	You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is called out-of-profile traffic.
Bandwidth	Specify the bandwidth in kilobit per second (Kbps). Enter a number between 1 and 1000000.
Out-of-Profile DSCP	Specify a new DSCP number (between 0 and 63) if you want to replace or remark the DSCP number for out-of-profile traffic.
Action Specify the action(s) the Switch takes on the associated classified traffic flow.	
Forwarding	Select **No change** to forward the packets. Select **Discard the packet** to drop the packets. Select **Do not drop the matching frame previously marked for dropping** to retain the frames that were marked to be dropped before.
Priority	Select **No change** to keep the priority setting of the frames. Select **Set the packet's 802.1p priority** to replace the packet's 802.1p priority field with the value you set in the Priority field. Select **Send the packet to priority queue** to put the packets in the designated queue. Select **Replace the 802.1p priority field with the IP TOS value** to replace the packet's 802.1p priority field with the value you set in the **TOS** field.
Diffserv	Select **No change** to keep the TOS and/or DSCP fields in the packets. Select **Set the packet's TOS field** to set the TOS field with the value you configure in the **TOS** field. Select **Replace the IP TOS with the 802.1p priority value** to replace the TOS field with the value you configure in the **Priority** field. Select **Set the Diffserv Codepoint field in the frame** to set the DSCP field with the value you configure in the **DSCP** field.
Outgoing	Select **Send the packet to the mirror port** to send the packet to the mirror port. Select **Send the packet to the egress port** to send the packet to the egress port.
Metering	Select **Enable** to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets.

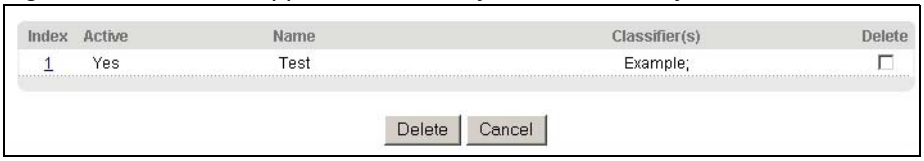
Table 58 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Out-of-profile action	Select the action(s) to be performed for out-of-profile traffic. Select **Drop the packet** to discard the out-of-profile traffic. Select **Change the DSCP value** to replace the DSCP field with the value specified in the **Out of profile DSCP** field. Select **Set Out-Drop Precedence** to mark out-of-profile traffic and drop it when network is congested. Select **Do not drop the matching frame previously marked for dropping** to queue the frames that are marked to be dropped.
Add	Click **Add** to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to set the above fields back to the factory defaults.

19.3 Viewing and Editing Policy Configuration

To view a summary of the classifier configuration, scroll down to the summary table at the bottom of the **Policy** screen. To change the settings of a rule, click a number in the **Index** field.

Figure 82 Advanced Application > Policy Rule: Summary Table



The following table describes the labels in this screen.

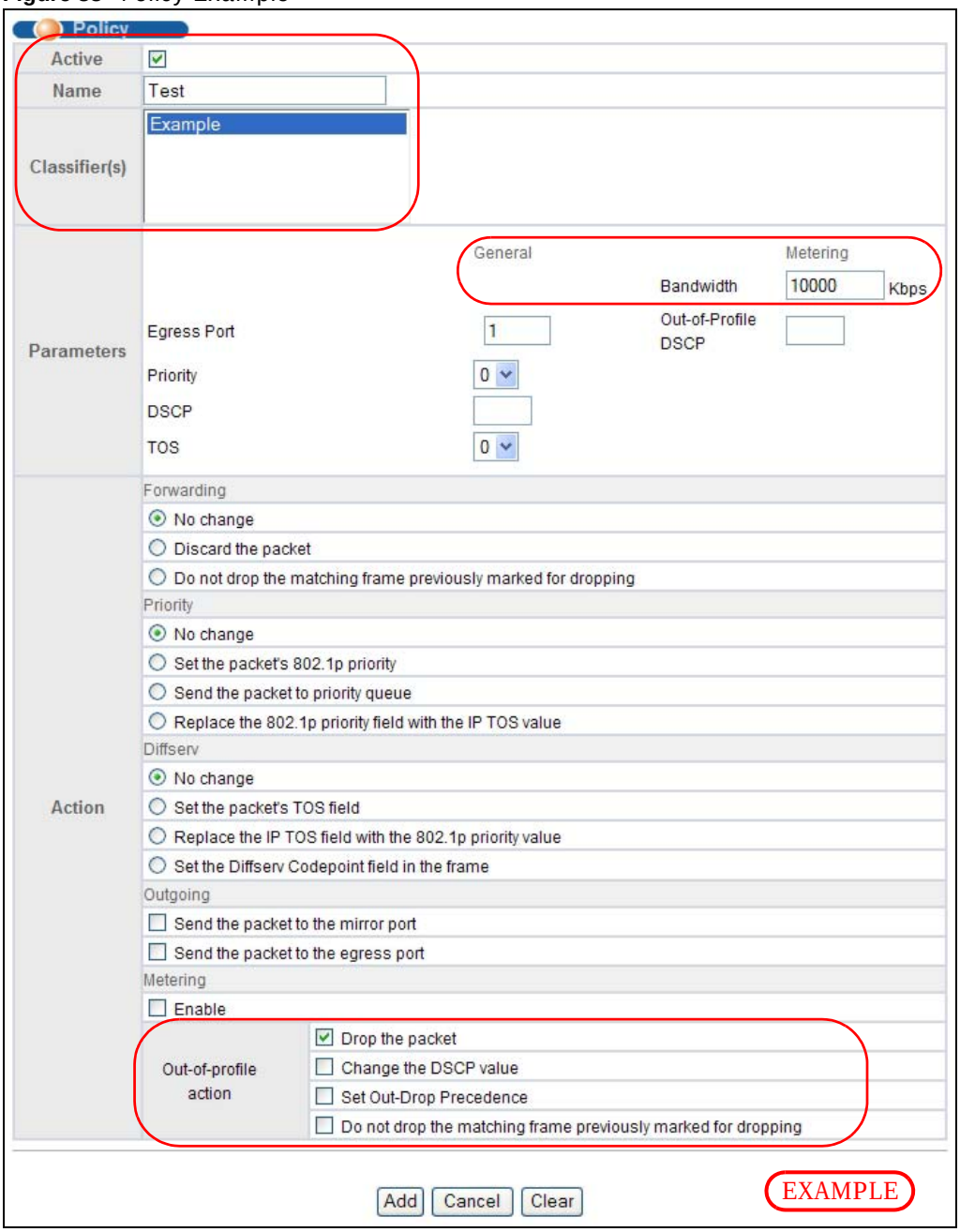
Table 59 Policy: Summary Table

LABEL	DESCRIPTION
Index	This field displays the policy index number. Click an index number to edit the policy.
Active	This field displays **Yes** when policy is activated and **No** when is it deactivated.
Name	This field displays the name you have assigned to this policy.
Classifier(s)	This field displays the name(s) of the classifier to which this policy applies.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

19.4 Policy Example

The figure below shows an example **Policy** screen where you configure a policy to limit bandwidth and discard out-of-profile traffic on a traffic flow classified using the **Example** classifier (refer to Section 18.4 on page 156).

Figure 83 Policy Example



20

Queuing Method

This chapter introduces the queuing methods supported.

20.1 Queuing Method Overview

Queuing is used to help solve performance degradation when there is network congestion. Use the **Queuing Method** screen to configure queuing algorithms for outgoing traffic. See also **Priority Queue Assignment** in **Switch Setup** and **802.1p Priority** in **Port Setup** for related information.

Queuing algorithms allow switches to maintain separate queues for packets from each individual source or flow and prevent a source from monopolizing the bandwidth.

20.1.1 Strictly Priority Queuing

Strictly Priority Queuing (SPQ) services queues based on priority only. As traffic comes into the Switch, traffic on the highest priority queue, Q7 is transmitted first. When that queue empties, traffic on the next highest-priority queue, Q6 is transmitted until Q6 empties, and then traffic is transmitted on Q5 and so on. If higher priority queues never empty, then traffic on lower priority queues never gets sent. SP does not automatically adapt to changing network requirements.

20.1.2 Weighted Fair Queuing

Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on its bandwidth weight (the number you configure in the **Weight** field) when there is traffic congestion. WFQ is activated only when a port has more traffic than it can handle. Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. By default, the weight for Q0 is 1, for Q1 is 2, for Q2 is 3, and so on.

The weights range from 1 to 15 and the actual guaranteed bandwidth is calculated as follows:

Weight x 2 KB

If the weight setting is 5, the actual quantum guaranteed to the associated queue would be as follows:

5 x 2KB = 10 KB

20.1.3 Weighted Round Robin Scheduling (WRR)

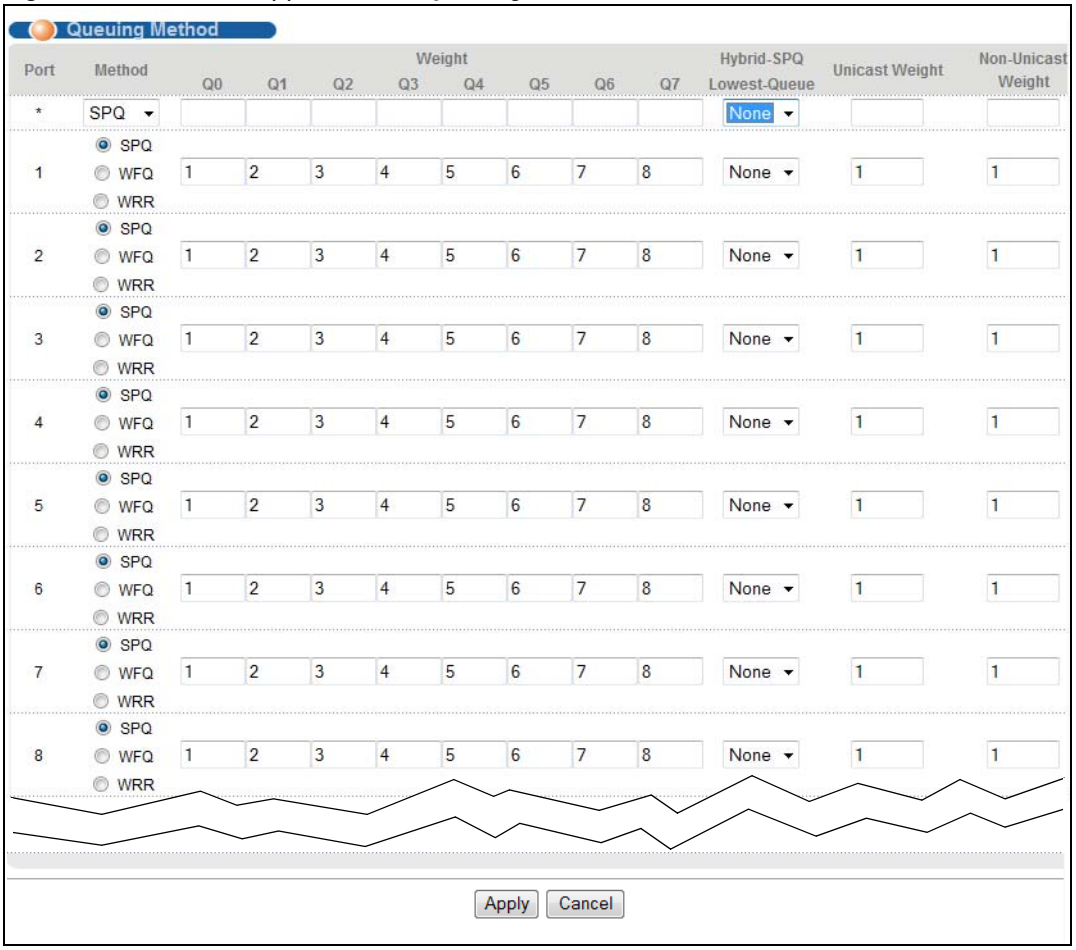
Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that port. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

Weighted Round Robin Scheduling (WRR) uses the same algorithm as round robin scheduling, but services queues based on their priority and queue weight (the number you configure in the queue **Weight** field) rather than a fixed amount of bandwidth. WRR is activated only when a port has more traffic than it can handle. Queues with larger weights get more service than queues with smaller weights. This queuing mechanism is highly efficient in that it divides any available bandwidth across the different traffic queues and returns to queues that have not yet emptied.

20.2 Configuring Queuing

Click **Advanced Application** > **Queuing Method** in the navigation panel.

Figure 84 Advanced Application > Queuing Method



The following table describes the labels in this screen.

Table 60 Advanced Application > Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Method	Select **SPQ** (Strictly Priority Queuing), **WFQ** (Weighted Fair Queuing) or **WRR** (Weighted Round Robin). Strictly Priority services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest. Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on their bandwidth weight (the number you configure in the **Weight** field). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. Weighted Round Robin Scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue **Weight** field). Queues with larger weights get more service than queues with smaller weights.
Weight Q0-Q7	When you select **WFQ** or **WRR** enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights.
Hybrid-SPQ Lowest-Queue	This field is applicable only when you select **WFQ** or **WRR**. Select a queue (**Q0** to **Q7**) to have the Switch use **SPQ** to service the subsequent queue(s) after and including the specified queue for the 1000Base-T, 1000Base-X and 10 Gigabit Ethernet ports. For example, if you select **Q5**, the Switch services traffic on **Q5**, **Q6** and **Q7** using **SPQ**. Select **None** to always use **WFQ** or **WRR**.
Unicast Weight	Enter a default weight for unicast traffic from this port. The weight is the ratio of unicast traffic to non-unicast traffic. The allowed range is from 1 to 127. For example, if 1 is entered for unicast traffic and 2 is entered for non-unicast, then two-thirds of the bandwidth on this port is available for non-unicast traffic.
Non-Unicast Weight	Enter a default weight for broadcast or multicast traffic from this port. The weight is the ratio of unicast traffic to non-unicast traffic. The allowed range is from 1 to 127. For example, if 1 is entered for unicast traffic and 2 is entered for non-unicast, then two-thirds of the bandwidth on this port is available for non-unicast traffic.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

21

VLAN Stacking

This chapter shows you how to configure VLAN stacking on your Switch. See the chapter on VLANs for more background information on Virtual LAN.

21.1 VLAN Stacking Overview

A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

Use VLAN stacking to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames (“double-tagged” frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different service, based on specific VLANs, for many different customers.

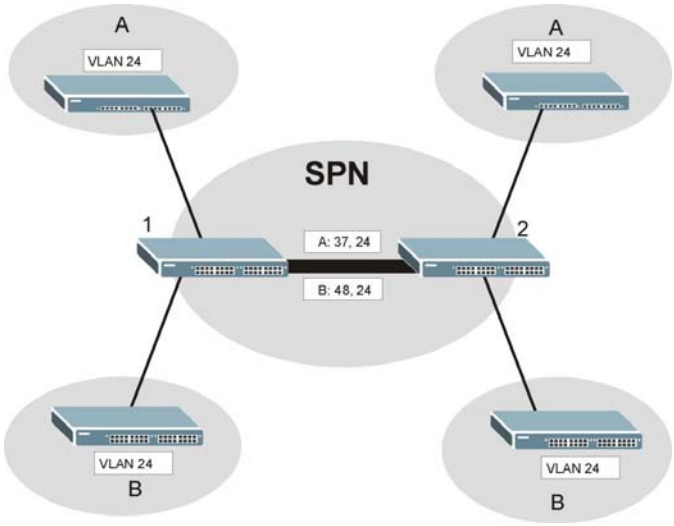
A service provider’s customers may require a range of VLANs to handle multiple applications. A service provider’s customers can assign their own inner VLAN tags on ports for these applications. The service provider can assign an outer VLAN tag for each customer. Therefore, there is no VLAN tag overlap among customers, so traffic from different customers is kept separate.

21.1.1 VLAN Stacking Example

In the following example figure, both **A** and **B** are Service Provider’s Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by

adding tag 37 to distinguish customer **A** and tag 48 to distinguish customer **B** at edge device **1** and then stripping those tags at edge device **2** as the data frames leave the network.

Figure 85 VLAN Stacking Example



21.2 VLAN Stacking Port Roles

Each port can have three VLAN stacking “roles”, **Normal**, **Access Port** and **Tunnel Port** (the latter is for Gigabit ports only).

- Select **Normal** for “regular” (non-VLAN stacking) IEEE 802.1Q frame switching.
- Select **Access Port** for ingress ports on the service provider's edge devices (**1** and **2** in the VLAN stacking example figure). The incoming frame is treated as "untagged", so a second VLAN tag (outer VLAN tag) can be added.

Note: Static VLAN **Tx Tagging** MUST be disabled on a port where you choose **Normal** or **Access Port**.

- Select **Tunnel Port** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. All VLANs belonging to a customer can be aggregated into a single service provider's VLAN (using the outer VLAN tag defined by the Service Provider’s (SP) VLAN ID (VID)).

Note: Static VLAN **Tx Tagging** MUST be enabled on a port where you choose **Tunnel Port**.

21.3 VLAN Tag Format

A VLAN tag (service provider VLAN stacking or customer IEEE 802.1Q) consists of the following three fields.

Table 61 VLAN Tag Format

Type	Priority	VID

Type is a standard Ethernet type code identifying the frame and indicates that whether the frame carries IEEE 802.1Q tag information. **SP TPID** (Service Provider Tag Protocol Identifier) is the service provider VLAN stacking tag type. Many vendors use 0x8100 or 0x9100.

TPID (Tag Protocol Identifier) is the customer IEEE 802.1Q tag.

- If the VLAN stacking port role is **Access Port**, then the Switch adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure).
- If the VLAN stacking port role is **Tunnel Port**, then the Switch only adds the **SP TPID** tag to all incoming frames on the service provider's edge devices (1 and 2 in the VLAN stacking example figure) that have an **SP TPID** different to the one configured on the Switch. (If an incoming frame's **SP TPID** is the same as the one configured on the Switch, then the Switch will not add the tag.)

Priority refers to the IEEE 802.1p standard that allows the service provider to prioritize traffic based on the class of service (CoS) the customer has paid for.

- On the Switch, configure priority level of the inner IEEE 802.1Q tag in the **Port Setup** screen.
- "0" is the lowest priority level and "7" is the highest.

VID is the VLAN ID. **SP VID** is the VID for the second (service provider's) VLAN tag.

21.3.1 Frame Format

The frame format for an untagged Ethernet frame, a single-tagged 802.1Q frame (customer) and a "double-tagged" 802.1Q frame (service provider) is shown next.

Configure the fields as highlighted in the Switch **VLAN Stacking** screen.

Table 62 Single and Double Tagged 802.11Q Frame Format

						DA	SA	Len/ Etype	Data	FCS	Untagged Ethernet frame
			DA	SA	**TPID**	**Priority**	**VID**	Len/ Etype	Data	FCS	IEEE 802.1Q customer tagged frame
DA	SA	**SPTPID**	**Priority**	**VID**	**TPID**	**Priority**	**VID**	Len/ Etype	Data	FCS	Double-tagged frame

Table 63 802.1Q Frame

DA	Destination Address	Priority	802.1p Priority
SA	Source Address	Len/ Etype	Length and type of Ethernet frame

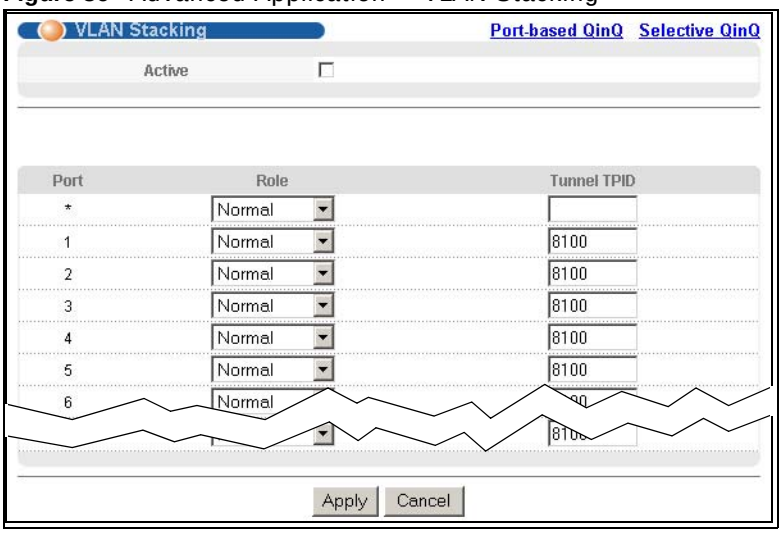
Table 63 802.1Q Frame

(SP)TPID	(Service Provider) Tag Protocol IDentifier	Data	Frame data
VID	VLAN ID	FCS	Frame Check Sequence

21.4 Configuring VLAN Stacking

Click **Advanced Applications > VLAN Stacking** to display the screen as shown.

Figure 86 Advanced Application > VLAN Stacking



The following table describes the labels in this screen.

Table 64 Advanced Application > VLAN Stacking

LABEL	DESCRIPTION
Active	Select this checkbox to enable VLAN stacking on the Switch.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Role	Select **Normal** to have the Switch ignore frames received (or transmitted) on this port with VLAN stacking tags. Anything you configure in **SPVID** and **Priority** of the **Port-based QinQ** or the **Selective QinQ** screen are ignored. Select **Access Port** to have the Switch add the SP TPID tag to all incoming frames received on this port. Select **Access Port** for ingress ports at the edge of the service provider's network. Select **Tunnel Port** (available for Gigabit ports only) for egress ports at the edge of the service provider's network. Select **Tunnel Port** to have the Switch add the **Tunnel TPID** tag to all outgoing frames sent on this port. In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.

Table 64 Advanced Application > VLAN Stacking (continued)

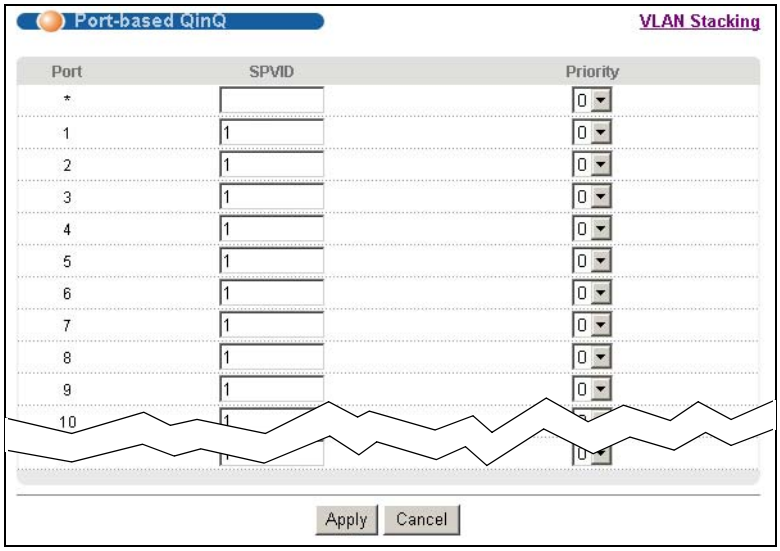
LABEL	DESCRIPTION
Tunnel TPID	TPID is a standard Ethernet type code identifying the frame and indicates whether the frame carries IEEE 802.1Q tag information. Enter a four-digit hexadecimal number from 0000 to FFFF that the Switch adds in the outer VLAN tag of the frames sent on the tunnel port(s). The Switch also uses this to check if the received frames are double-tagged. The value of this field is 0x8100 as defined in IEEE 802.1Q. If the Switch needs to communicate with other vendors' devices, they should use the same TPID. Note: You can define up to four different tunnel TPIDs (including **8100**) in this screen at a time.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

21.4.1 Port-based Q-in-Q

Port-based Q-in-Q lets the Switch treat all frames received on the same port as the same VLAN flows and add the same outer VLAN tag to them, even they have different customer VLAN IDs.

Click **Port-based QinQ** in the **Advanced Application > VLAN Stacking** screen to display the screen as shown.

Figure 87 Advanced Application > VLAN Stacking > Port-based QinQ



The following table describes the labels in this screen.

Table 65 Advanced Application > VLAN Stacking > Port-based QinQ

LABEL	DESCRIPTION
Port	The port number identifies the port you are configuring.
SPVID	**SPVID** is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See Chapter 7 on page 81 for more background information on VLAN ID.

Table 65 Advanced Application > VLAN Stacking > Port-based QinQ (continued)

LABEL	DESCRIPTION
Priority	Select a priority level (from 0 to 7). This is the service provider's priority level that adds to the frames received on this port. "0" is the lowest priority level and "7" is the highest.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

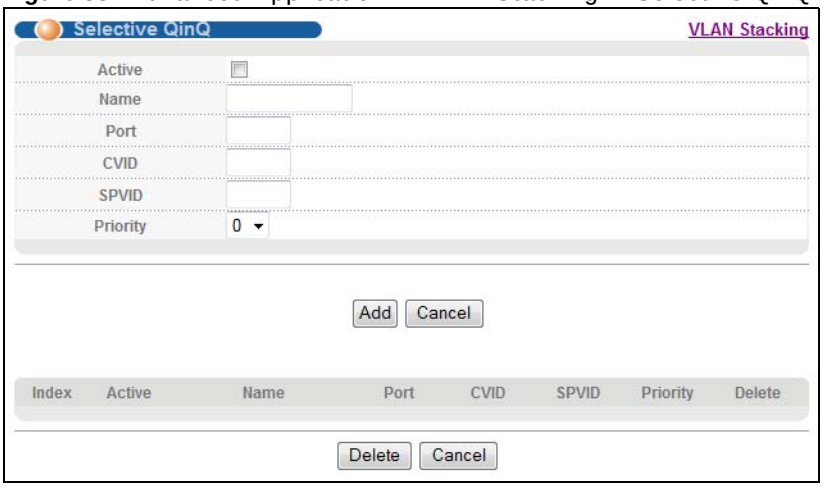
21.4.2 Selective Q-in-Q

Selective Q-in-Q is VLAN-based. It allows the Switch to add different outer VLAN tags to the incoming frames received on one port according to their inner VLAN tags.

Note: Selective Q-in-Q rules are only applied to single-tagged frames received on the access ports. If the incoming frames are untagged or single-tagged but received on a tunnel port or cannot match any selective Q-in-Q rules, the Switch applies the port-based Q-in-Q rules to them.

Click **Selective QinQ** in the **Advanced Application > VLAN Stacking** screen to display the screen as shown.

Figure 88 Advanced Application > VLAN Stacking > Selective QinQ



The following table describes the labels in this screen.

Table 66 Advanced Application > VLAN Stacking > Selective QinQ

LABEL	DESCRIPTION
Active	Check this box to activate this rule.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Port	The port number identifies the port you are configuring.
CVID	Enter a customer VLAN ID (the inner VLAN tag) from 1 to 4094. This is the VLAN tag carried in the packets from the subscribers.

Table 66 Advanced Application > VLAN Stacking > Selective QinQ (continued)

LABEL	DESCRIPTION
SPVID	**SPVID** is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See Chapter 7 on page 81 for more background information on VLAN ID.
Priority	Select a priority level (from 0 to 7). This is the service provider's priority level that adds to the frames received on this port. "0" is the lowest priority level and "7" is the highest.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Index	This is the number of the selective VLAN stacking rule.
Active	This shows whether this rule is activated or not.
Name	This is the descriptive name for this rule.
Port	This is the port number to which this rule is applied.
CVID	This is the customer VLAN ID in the incoming packets.
SPVID	This is the service provider's VLAN ID that adds to the packets from the subscribers.
Priority	This is the service provider's priority level in the packets.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

22

Multicast

This chapter shows you how to configure various multicast features.

22.1 Multicast Overview

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

22.1.1 IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different subnetwork. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA website for more information).

22.1.2 IGMP Filtering

With the IGMP filtering feature, you can control which IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

You can set the Switch to filter the multicast group join reports on a per-port basis by configuring an IGMP filtering profile and associating the profile to a port.

22.1.3 IGMP Snooping

The Switch can passively snoop on IGMP packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the Switch to learn multicast groups without you having to manually configure them.

The Switch forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your Switch.

22.1.4 IGMP Snooping and VLANs

The Switch can perform IGMP snooping on up to 16 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first 16 VLANs that send IGMP packets. This is referred to as auto mode. Alternatively, you can specify the VLANs that IGMP snooping should be performed on. This is referred to as fixed mode. In fixed mode the Switch does not learn multicast group membership of any VLANs other than those explicitly added as an IGMP snooping VLAN.

22.2 Multicast Status

Click **Advanced Applications > Multicast** to display the screen as shown. This screen shows the multicast group information. See Section 22.1 on page 172 for more information on multicasting.

Figure 89 Advanced Application > Multicast

The following table describes the labels in this screen.

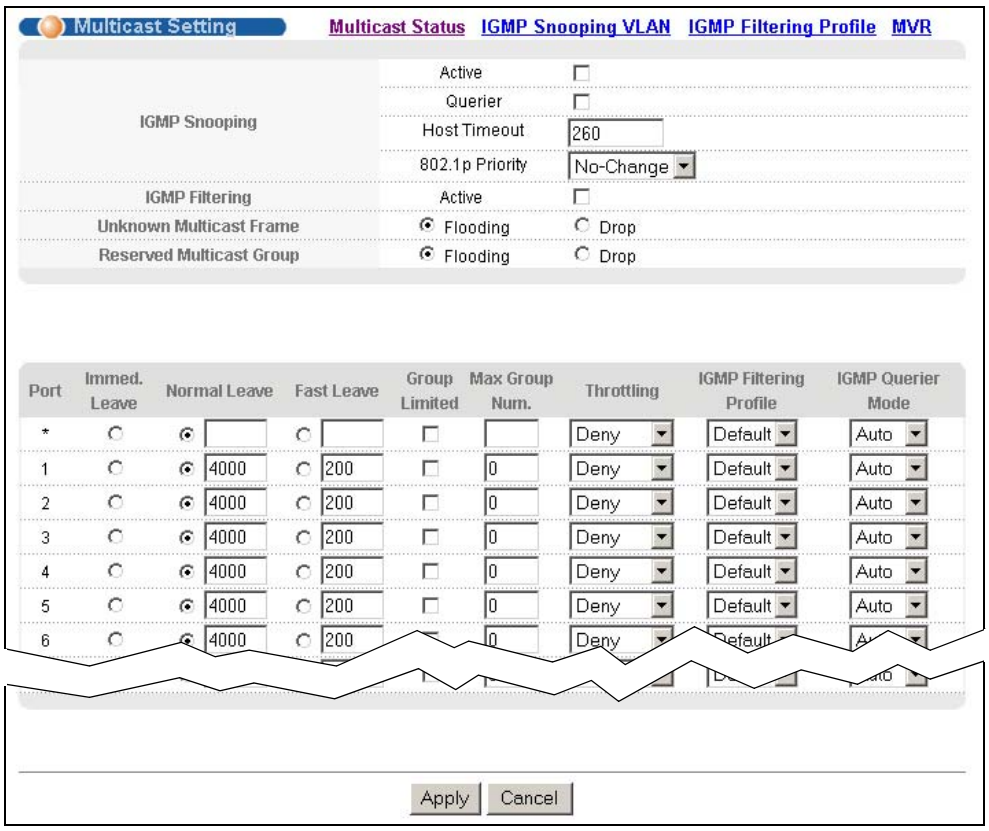
Table 67 Multicast Status

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.

22.3 Multicast Setting

Click **Advanced Applications > Multicast > Multicast Setting** link to display the screen as shown. See Section 22.1 on page 172 for more information on multicasting.

Figure 90 Advanced Application > Multicast > Multicast Setting



The following table describes the labels in this screen.

Table 68 Advanced Application > Multicast > Multicast Setting

LABEL	DESCRIPTION
IGMP Snooping	Use these settings to configure IGMP Snooping.
Active	Select **Active** to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.
Querier	Select this option to allow the Switch to send IGMP General Query messages to the VLANs with the multicast hosts attached.
Host Timeout	Specify the time (from 1 to 16 711 450) in seconds that elapses before the Switch removes an IGMP group membership entry if it does not receive report messages from the port.
802.1p Priority	Select a priority level (0-7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select **No-Change** to not replace the priority.
IGMP Filtering	Select **Active** to enable IGMP filtering to control which IGMP groups a subscriber on a port can join. Note: If you enable IGMP filtering, you must create and assign IGMP filtering profiles for the ports that you want to allow to join multicast groups.

Table 68 Advanced Application > Multicast > Multicast Setting (continued)

LABEL	DESCRIPTION
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Reserved Multicast Group	The IP address range of 224.0.0.0 to 224.0.0.255 are reserved for multicasting on the local network only. For example, 224.0.0.1 is for all hosts on a local network segment and 224.0.0.9 is used to send RIP routing information to all RIP v2 routers on the same network segment. A multicast router will not forward a packet with the destination IP address within this range to other networks. See the IANA web site for more information. The layer-2 multicast MAC addresses used by Cisco layer-2 protocols, 01:00:0C:CC:CC:CC and 01:00:0C:CC:CC:CD, are also included in this group. Specify the action to perform when the Switch receives a frame with a reserved multicast address. Select **Drop** to discard the frame(s). Select **Flooding** to send the frame(s) to all ports.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Immed. Leave	Select this option to set the Switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.
Normal Leave	Enter an IGMP normal leave timeout value (from 200 to 6,348,800) in miliseconds. Select this option to have the Switch use this timeout to update the forwarding table for the port. In normal leave mode, when the Switch receives an IGMP leave message from a host on a port, it forwards the message to the multicast router. The multicast router then sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. The Switch forwards the query message to all hosts connected to the port and waits for IGMP reports from hosts to update the forwarding table. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.
Fast Leave	Enter an IGMP fast leave timeout value (from 200 to 6,348,800) in miliseconds. Select this option to have the Switch use this timeout to update the forwarding table for the port. In fast leave mode, right after receiving an IGMP leave message from a host on a port, the Switch itself sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. This helps speed up the leave process. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.

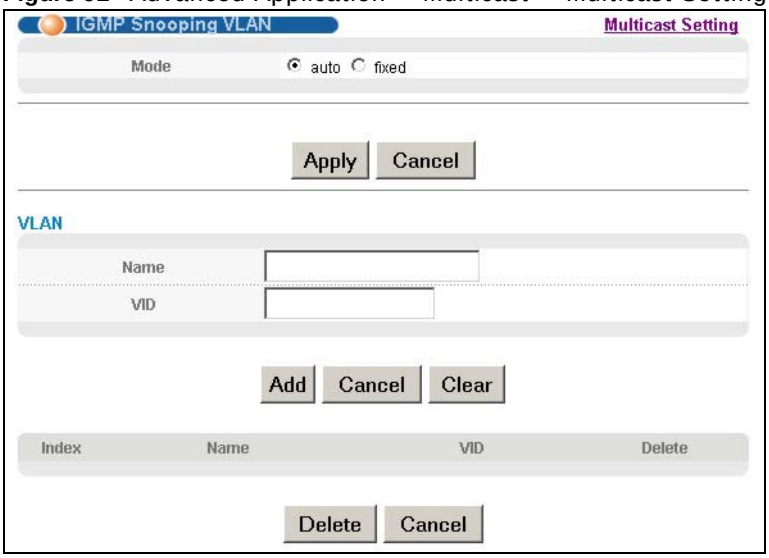
Table 68 Advanced Application > Multicast > Multicast Setting (continued)

LABEL	DESCRIPTION
Throttling	IGMP throttling controls how the Switch deals with the IGMP reports when the maximum number of the IGMP groups a port can join is reached. Select **Deny** to drop any new IGMP join report received on this port until an existing multicast forwarding table entry is aged out. Select **Replace** to replace an existing entry in the multicast forwarding table with the new IGMP report(s) received on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select **Default** to prohibit the port from joining any multicast group. You can create IGMP filtering profiles in the **Multicast** > **Multicast Setting** > **IGMP Filtering Profile** screen.
IGMP Querier Mode	The Switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The Switch forwards IGMP join or leave packets to an IGMP query port. Select **Auto** to have the Switch use the port as an IGMP query port if the port receives IGMP query packets. Select **Fixed** to have the Switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select **Edge** to stop the Switch from using the port as an IGMP query port. The Switch will not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

22.4 IGMP Snooping VLAN

Click **Advanced Applications > Multicast** in the navigation panel. Click the **Multicast Setting** link and then the **IGMP Snooping VLAN** link to display the screen as shown. See Section 22.1.4 on page 173 for more information on IGMP Snooping VLAN.

Figure 91 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN



The following table describes the labels in this screen.

Table 69 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN

LABEL	DESCRIPTION
Mode	Select **auto** to have the Switch learn multicast group membership information of any VLANs automatically. Select **fixed** to have the Switch only learn multicast group membership information of the VLAN(s) that you specify below. In either **auto** or **fixed** mode, the Switch can learn up to 16 VLANs (including up to five VLANs you configured in the **MVR** screen). For example, if you have configured one multicast VLAN in the **MVR** screen, you can only specify up to 15 VLANs in this screen. The Switch drops any IGMP control messages which do not belong to these 16 VLANs. Note: You must also enable IGMP snooping in the **Multicast Setting** screen first.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
VLAN	Use this section of the screen to add VLANs upon which the Switch is to perform IGMP snooping.
Name	Enter the descriptive name of the VLAN for identification purposes.
VID	Enter the ID of a static VLAN; the valid range is between 1 and 4094. Note: You cannot configure the same VLAN ID as in the **MVR** screen.

Table 69 Advanced Application > Multicast > Multicast Setting > IGMP Snooping VLAN (continued)

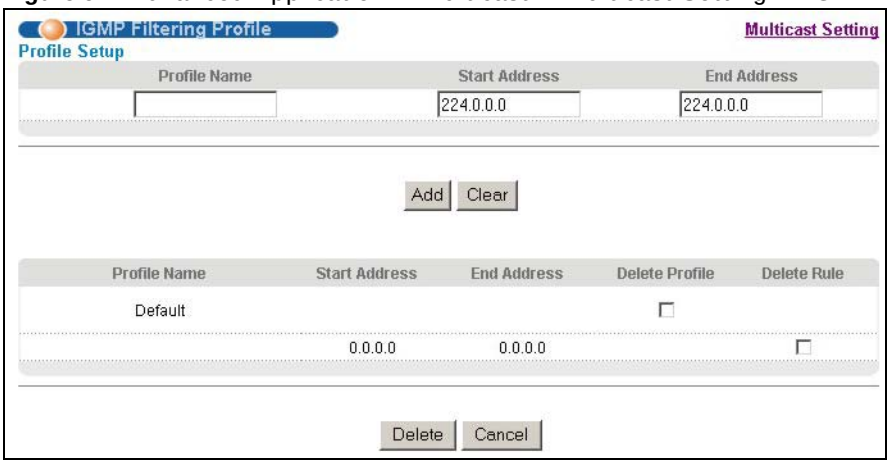
LABEL	DESCRIPTION
Add	Click **Add** to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is the number of the IGMP snooping VLAN entry in the table.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
Delete	Check the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

22.5 IGMP Filtering Profile

An IGMP filtering profile specifies a range of multicast groups that clients connected to the Switch are able to join. A profile contains a range of multicast IP addresses which you want clients to be able to join. Profiles are assigned to ports (in the **Multicast Setting** screen). Clients connected to those ports are then able to join the multicast groups specified in the profile. Each port can be assigned a single profile. A profile can be assigned to multiple ports.

Click **Advanced Applications** > **Multicast** > **Multicast Setting** > **IGMP Filtering Profile** link to display the screen as shown.

Figure 92 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile



The following table describes the labels in this screen.

Table 70 Advanced Application > Multicast > Multicast Setting > IGMP Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Type the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the **Start Address** and **End Address** fields.
Add	Click **Add** to save the profile to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click **Clear** to reset the fields to the factory defaults.
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast address range.
End Address	This field displays the end of the multicast address range.
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the **Delete Profile** column, then click the **Delete** button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the **Delete Rule** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete Profile**/**Delete Rule** check boxes.

22.6 MVR Overview

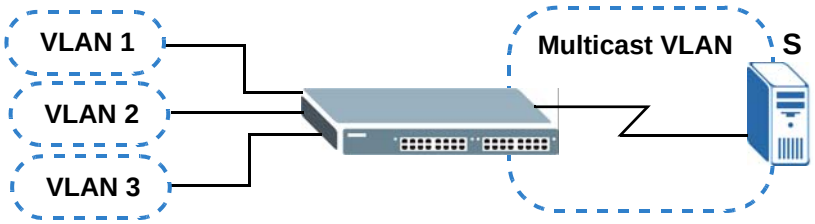
Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. While isolated in different subscriber VLANs, connected devices can subscribe to and unsubscribe from the multicast stream in the multicast VLAN. This improves bandwidth utilization with reduced multicast traffic in the subscriber VLANs and simplifies multicast group management.

MVR only responds to IGMP join and leave control messages from multicast groups that are configured under MVR. Join and leave reports from other multicast groups are managed by IGMP snooping.

The following figure shows a network example. The subscriber VLAN (**1**, **2** and **3**) information is hidden from the streaming media server, **S**. In addition, the multicast VLAN information is only visible to the Switch and **S**.

Figure 93 MVR Network Example



22.6.1 Types of MVR Ports

In MVR, a source port is a port on the Switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast traffic. Once configured, the Switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

22.6.2 MVR Modes

You can set your Switch to operate in either dynamic or compatible mode.

In dynamic mode, the Switch sends IGMP leave and join reports to the other multicast devices (such as multicast routers or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding table to forward or not forward multicast traffic to the receiver ports.

In compatible mode, the Switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

22.6.3 How MVR Works

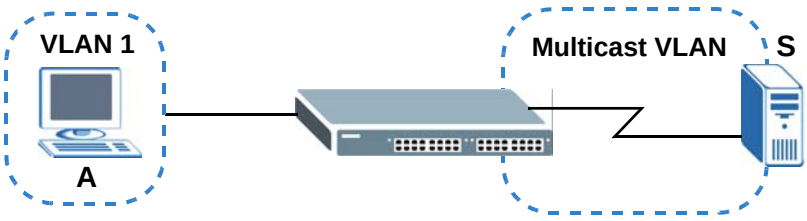
The following figure shows a multicast television example where a subscriber device (such as a computer) in VLAN 1 receives multicast traffic from the streaming media server, **S**, via the Switch. Multiple subscriber devices can connect through a port configured as the receiver on the Switch.

When the subscriber selects a television channel, computer **A** sends an IGMP report to the Switch to join the appropriate multicast group. If the IGMP report matches one of the configured MVR multicast group addresses on the Switch, an entry is created in the forwarding table on the Switch. This maps the subscriber VLAN to the list of forwarding destinations for the specified multicast traffic.

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the Switch to leave the multicast group. The Switch sends a query to VLAN 1 on the receiver port (in this case, an uplink port on the Switch). If there is another subscriber device connected to this

port in the same subscriber VLAN, the receiving port will still be on the list of forwarding destination for the multicast traffic. Otherwise, the Switch removes the receiver port from the forwarding table.

Figure 94 MVR Multicast Television Example



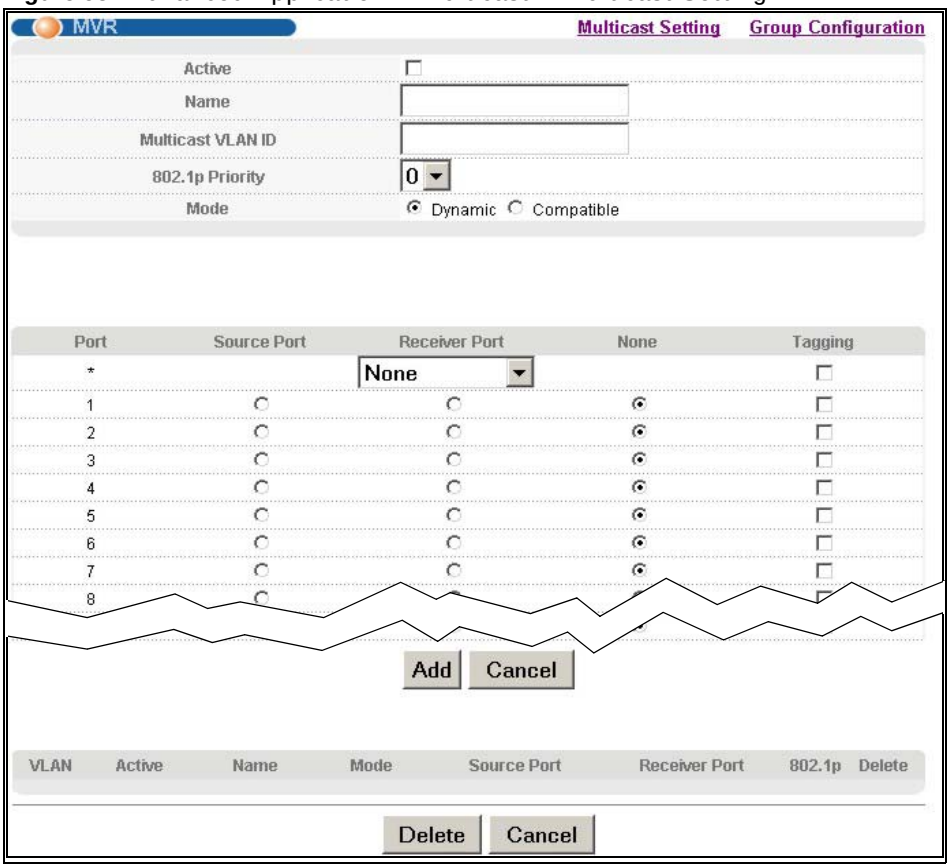
22.7 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN. Click **Advanced Applications > Multicast** > **Multicast Setting > MVR** link to display the screen as shown next.

Note: You can create up to five multicast VLANs and up to 256 multicast rules on the Switch.

Note: Your Switch automatically creates a static VLAN (with the same VID) when you create a multicast VLAN in this screen.

Figure 95 Advanced Application > Multicast > Multicast Setting > MVR



The following table describes the related labels in this screen.

Table 71 Advanced Application > Multicast > Multicast Setting > MVR

LABEL	DESCRIPTION
Active	Select this check box to enable MVR to allow one single multicast VLAN to be shared among different subscriber VLANs on the network.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
802.1p Priority	Select a priority level (0-7) with which the Switch replaces the priority in outgoing IGMP control packets (belonging to this multicast VLAN).
Mode	Specify the MVR mode on the Switch. Choices are **Dynamic** and **Compatible**. Select **Dynamic** to send IGMP reports to all MVR source ports in the multicast VLAN. Select **Compatible** to set the Switch not to send IGMP reports.
Port	This field displays the port number on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 71 Advanced Application > Multicast > Multicast Setting > MVR (continued)

LABEL	DESCRIPTION
Source Port	Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
802.1p	This field displays the priority level.
Delete	To delete a multicast VLAN(s), select the rule(s) that you want to remove in the **Delete** column, then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

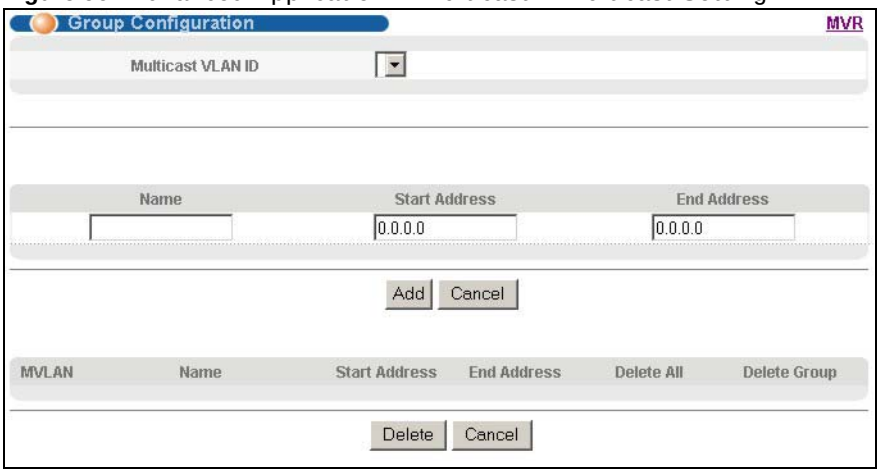
22.8 MVR Group Configuration

All source ports and receiver ports belonging to a multicast group can receive multicast data sent to this multicast group.

Configure MVR IP multicast group address(es) in the **Group Configuration** screen. Click **Group Configuration** in the **MVR** screen.

Note: A port can belong to more than one multicast VLAN. However, IP multicast group addresses in different multicast VLANs cannot overlap.

Figure 96 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration



The following table describes the labels in this screen.

Table 72 Advanced Application > Multicast > Multicast Setting > MVR: Group Configuration

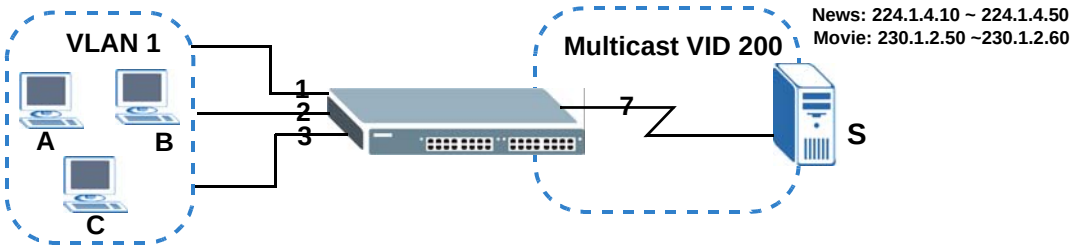
LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the **MVR** screen) from the drop-down list box.
Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to Section 22.1.1 on page 172 for more information on IP multicast addresses.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the **Start Address** field if you want to configure only one IP address for a multicast group. Refer to Section 22.1.1 on page 172 for more information on IP multicast addresses.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
MVLAN	This field displays the multicast VLAN ID.
Name	This field displays the descriptive name for this setting.
Start Address	This field displays the starting IP address of the multicast group.
End Address	This field displays the ending IP address of the multicast group.
Delete	Select **Delete All** or **Delete Group** and click **Delete** to remove the selected entry(ies) from the table.
Cancel	Select **Cancel** to clear the checkbox(es) in the table.

22.8.1 MVR Configuration Example

The following figure shows a network example where ports 1, 2 and 3 on the Switch belong to VLAN 1. In addition, port 7 belongs to the multicast group with VID 200 to receive multicast traffic (the

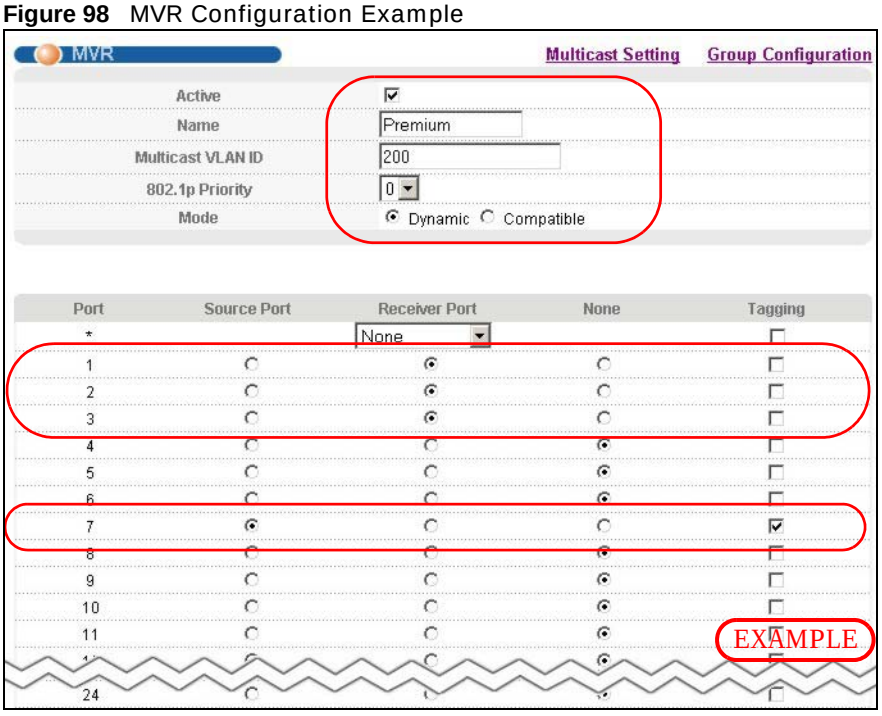
News and **Movie** channels) from the remote streaming media server, **S**. Computers A, B and C in VLAN 1 are able to receive the traffic.

Figure 97 MVR Configuration Example



To configure the MVR settings on the Switch, create a multicast group in the **MVR** screen and set the receiver and source ports.

Figure 98 MVR Configuration Example



To set the Switch to forward the multicast group traffic to the subscribers, configure multicast group settings in the **Group Configuration** screen. The following figure shows an example where two multicast groups (**News** and **Movie**) are configured for the multicast VLAN 200.

Figure 99 MVR Group Configuration Example

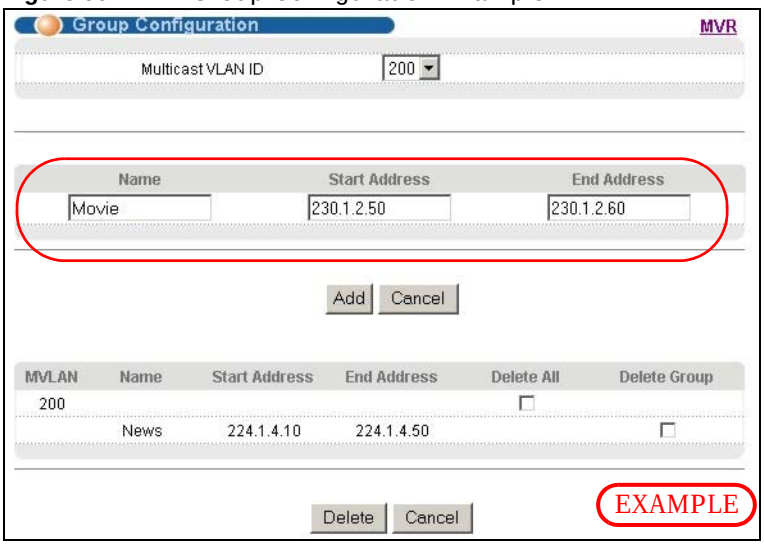
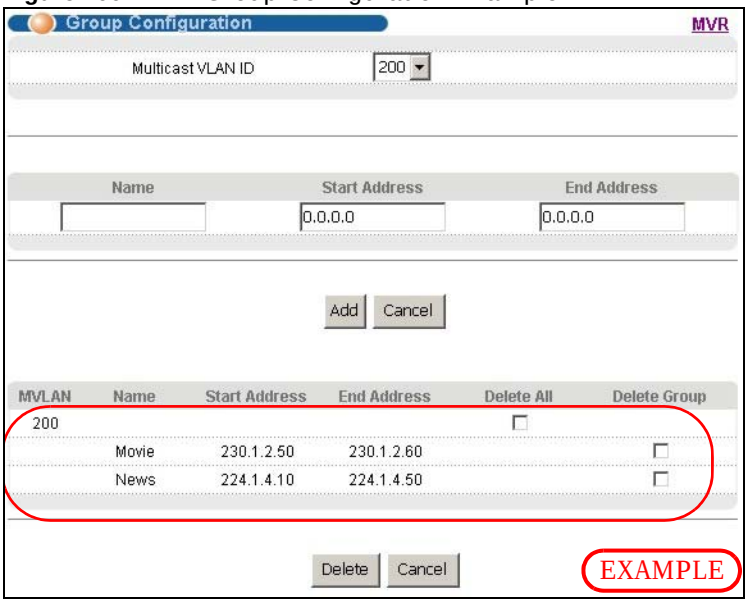


Figure 100 MVR Group Configuration Example



23

AAA

This chapter describes how to configure authentication, authorization and accounting settings on the Switch.

23.1 Authentication, Authorization and Accounting (AAA)

Authentication is the process of determining who a user is and validating access to the Switch. The Switch can authenticate users who try to log in based on user accounts configured on the Switch itself. The Switch can also use an external authentication server to authenticate a large number of users.

Authorization is the process of determining what a user is allowed to do. Different user accounts may have higher or lower privilege levels associated with them. For example, user A may have the right to create new login accounts on the Switch but user B cannot. The Switch can authorize users based on user accounts configured on the Switch itself or it can use an external server to authorize a large number of users.

Accounting is the process of recording what a user is doing. The Switch can use an external server to track when users log in, log out, execute commands and so on. Accounting can also record system related actions such as boot up and shut down times of the Switch.

The external servers that perform authentication, authorization and accounting functions are known as AAA servers. The Switch supports RADIUS (Remote Authentication Dial-In User Service, see Section 23.1.2 on page 188) and TACACS+ (Terminal Access Controller Access-Control System Plus, see Section 23.1.2 on page 188) as external authentication, authorization and accounting servers.

Figure 101 AAA Server

23.1.1 Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate and authorize users without interacting with a network AAA server. However, there is a limit on the number of users you may authenticate in this way (See Chapter 36 on page 276).

23.1.2 RADIUS and TACACS+

RADIUS and TACACS+ are security protocols used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS and TACACS+ authentication both allow you to validate an unlimited number of users from a central location.

The following table describes some key differences between RADIUS and TACACS+.

Table 73 RADIUS vs TACACS+

	RADIUS	TACACS+
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the client (the Switch) and the TACACS server is encrypted.

23.2 AAA Screens

The **AAA** screens allow you to enable authentication, authorization, accounting or all of them on the Switch. First, configure your authentication and accounting server settings (RADIUS, TACACS+ or both) and then set up the authentication priority, activate authorization and configure accounting settings.

Click **Advanced Application** > **AAA** in the navigation panel to display the screen as shown.

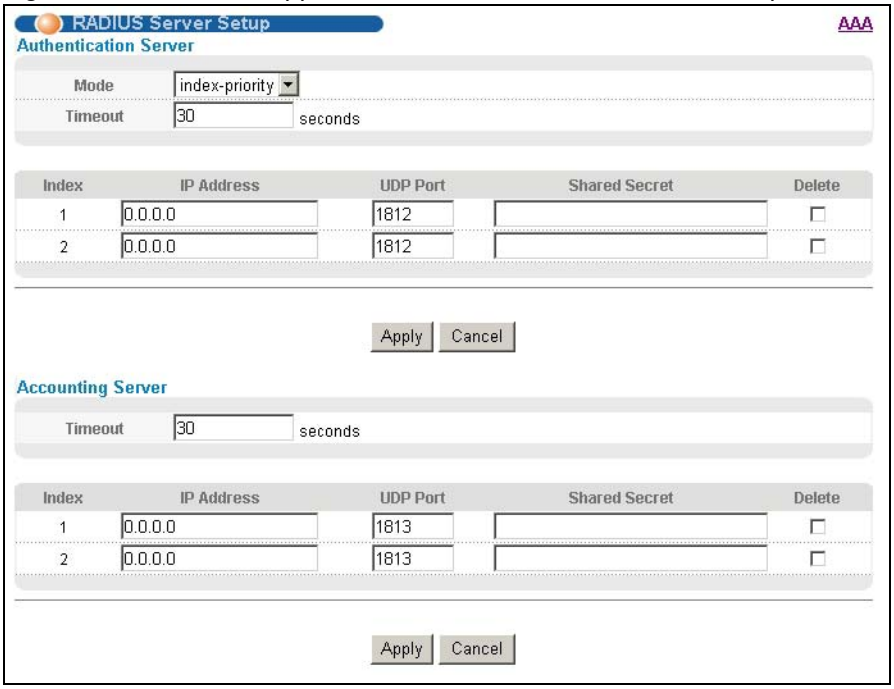
Figure 102 Advanced Application > AAA

23.2.1 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. See Section 23.1.2 on page 188 for more information on RADIUS servers and Section 23.3 on page 196 for RADIUS attributes utilized by the

authentication and accounting features on the Switch. Click on the **RADIUS Server Setup** link in the **AAA** screen to view the screen as shown.

Figure 103 Advanced Application > AAA > RADIUS Server Setup



The following table describes the labels in this screen.

Table 74 Advanced Application > AAA > RADIUS Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your RADIUS authentication settings.
Mode	This field only applies if you configure multiple RADIUS servers. Select **index-priority** and the Switch tries to authenticate with the first configured RADIUS server, if the RADIUS server does not respond then the Switch tries to authenticate with the second RADIUS server. Select **round-robin** to alternate between the RADIUS servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the RADIUS server. If you are using two RADIUS servers then the timeout value is divided between the two RADIUS servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first RADIUS server for 15 seconds and then tries the second RADIUS server.
Index	This is a read-only number representing a RADIUS server entry.
IP Address	Enter the IP address of an external RADIUS server in dotted decimal notation.
UDP Port	The default port of a RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the Switch.

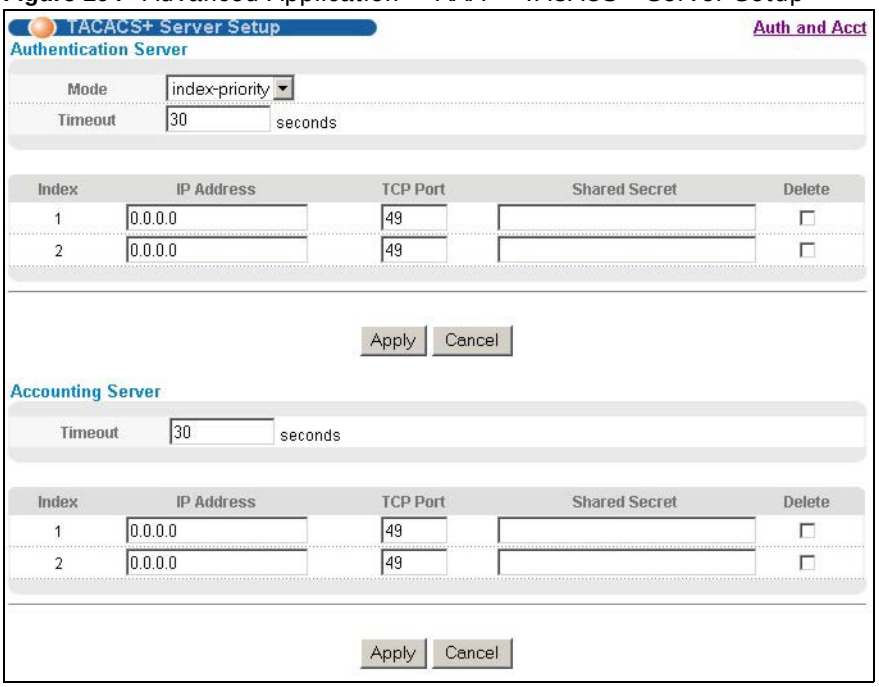
Table 74 Advanced Application > AAA > RADIUS Server Setup (continued)

LABEL	DESCRIPTION
Delete	Check this box if you want to remove an existing RADIUS server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Accounting Server	Use this section to configure your RADIUS accounting server settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the RADIUS accounting server.
Index	This is a read-only number representing a RADIUS accounting server entry.
IP Address	Enter the IP address of an external RADIUS accounting server in dotted decimal notation.
UDP Port	The default port of a RADIUS accounting server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS accounting server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS accounting server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS accounting server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.2.2 TACACS+ Server Setup

Use this screen to configure your TACACS+ server settings. See Section 23.1.2 on page 188 for more information on TACACS+ servers. Click on the **TACACS+ Server Setup** link in the **Authentication and Accounting** screen to view the screen as shown.

Figure 104 Advanced Application > AAA > TACACS+ Server Setup



The following table describes the labels in this screen.

Table 75 Advanced Application > AAA > TACACS+ Server Setup

LABEL	DESCRIPTION
Authentication Server	Use this section to configure your TACACS+ authentication settings.
Mode	This field is only valid if you configure multiple TACACS+ servers. Select **index-priority** and the Switch tries to authenticate with the first configured TACACS+ server, if the TACACS+ server does not respond then the Switch tries to authenticate with the second TACACS+ server. Select **round-robin** to alternate between the TACACS+ servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the TACACS+ server. If you are using two TACACS+ servers then the timeout value is divided between the two TACACS+ servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first TACACS+ server for 15 seconds and then tries the second TACACS+ server.
Index	This is a read-only number representing a TACACS+ server entry.
IP Address	Enter the IP address of an external TACACS+ server in dotted decimal notation.
TCP Port	The default port of a TACACS+ server for authentication is **49**. You need not change this value unless your network administrator instructs you to do so.

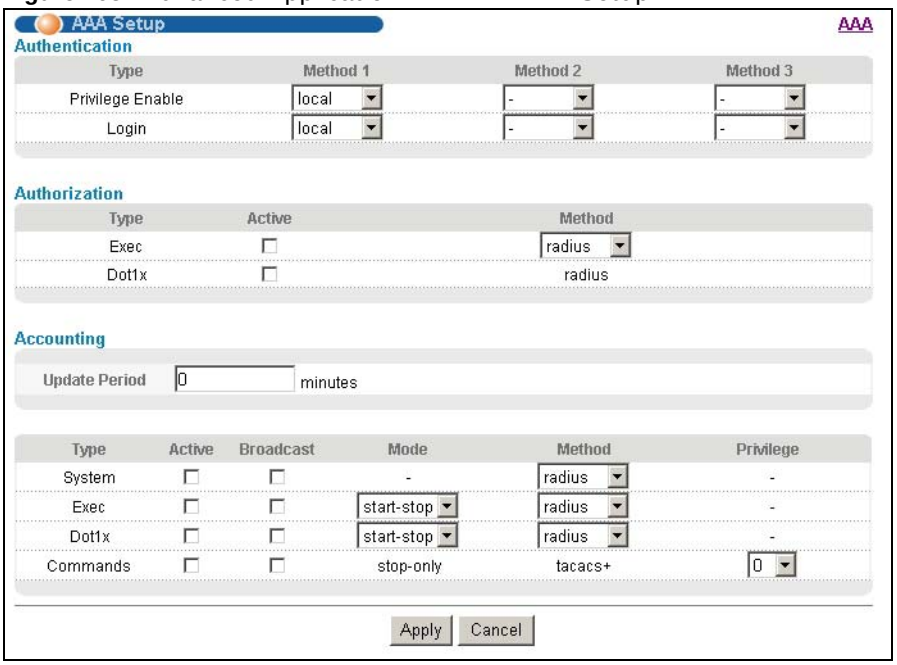
Table 75 Advanced Application > AAA > TACACS+ Server Setup (continued)

LABEL	DESCRIPTION
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Accounting Server	Use this section to configure your TACACS+ accounting settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the TACACS+ server.
Index	This is a read-only number representing a TACACS+ accounting server entry.
IP Address	Enter the IP address of an external TACACS+ accounting server in dotted decimal notation.
TCP Port	The default port of a TACACS+ accounting server is **49**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ accounting server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ accounting server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ accounting server entry from the Switch. This entry is deleted when you click **Apply**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.2.3 AAA Setup

Use this screen to configure authentication, authorization and accounting settings on the Switch. Click on the **AAA Setup** link in the **AAA** screen to view the screen as shown.

Figure 105 Advanced Application > AAA > AAA Setup



The following table describes the labels in this screen.

Table 76 Advanced Application > AAA > AAA Setup

LABEL	DESCRIPTION
Authentication	Use this section to specify the methods used to authenticate users accessing the Switch.
Privilege Enable	These fields specify which database the Switch should use (first, second and third) to authenticate access privilege level for administrator accounts (users for Switch management). Configure the access privilege of accounts via commands (see the Ethernet Switch CLI Reference Guide) for **local** authentication. The **TACACS+** and **RADIUS** are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first. You can specify up to three methods for the Switch to authenticate the access privilege level of administrators. The Switch checks the methods in the order you configure them (first **Method 1**, then **Method 2** and finally **Method 3**). You must configure the settings in the **Method 1** field. If you want the Switch to check other sources for access privilege level specify them in **Method 2** and **Method 3** fields. Select **local** to have the Switch check the access privilege configured for local authentication. Select **radius** or **tacacs+** to have the Switch check the access privilege via the external servers.

Table 76 Advanced Application > AAA > AAA Setup (continued)

LABEL	DESCRIPTION
Login	These fields specify which database the Switch should use (first, second and third) to authenticate administrator accounts (users for Switch management). Configure the local user accounts in the **Access Control > Logins** screen. The TACACS+ and RADIUS are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first. You can specify up to three methods for the Switch to authenticate administrator accounts. The Switch checks the methods in the order you configure them (first **Method 1**, then **Method 2** and finally **Method 3**). You must configure the settings in the **Method 1** field. If you want the Switch to check other sources for administrator accounts, specify them in **Method 2** and **Method 3** fields. Select **local** to have the Switch check the administrator accounts configured in the **Access Control > Logins** screen. Select **radius** to have the Switch check the administrator accounts configured via the RADIUS Server. Select **tacacs+** to have the Switch check the administrator accounts configured via the TACACS+ Server**.**
Authorization	Use this section to configure authorization settings on the Switch.
Type	Set whether the Switch provides the following services to a user. • **Exec**: Allow an administrator which logs in the Switch through Telnet or SSH to have different access privilege level assigned via the external server. • **Dot1x**: Allow an IEEE 802.1x client to have different bandwidth limit or VLAN ID assigned via the external server.
Active	Select this to activate authorization for a specified event types.
Method	Select whether you want to use RADIUS or TACACS+ for authorization of specific types of events. RADIUS is the only method for IEEE 802.1x authorization.
Accounting	Use this section to configure accounting settings on the Switch.
Update Period	This is the amount of time in minutes before the Switch sends an update to the accounting server. This is only valid if you select the **start-stop** option for the **Exec** or **Dot1x** entries.
Type	The Switch supports the following types of events to be sent to the accounting server(s): • **System** - Configure the Switch to send information when the following system events occur: system boots up, system shuts down, system accounting is enabled, system accounting is disabled • **Exec** - Configure the Switch to send information when an administrator logs in and logs out via the console port, telnet or SSH. • **Dot1x** - Configure the Switch to send information when an IEEE 802.1x client begins a session (authenticates via the Switch), ends a session as well as interim updates of a session. • **Commands** - Configure the Switch to send information when commands of specified privilege level and higher are executed on the Switch.
Active	Select this to activate accounting for a specified event types.
Broadcast	Select this to have the Switch send accounting information to all configured accounting servers at the same time. If you don't select this and you have two accounting servers set up, then the Switch sends information to the first accounting server and if it doesn't get a response from the accounting server then it tries the second accounting server.

Table 76 Advanced Application > AAA > AAA Setup (continued)

LABEL	DESCRIPTION
Mode	The Switch supports two modes of recording login events. Select: • **start-stop** - to have the Switch send information to the accounting server when a user begins a session, during a user's session (if it lasts past the **Update Period**), and when a user ends a session. • **stop-only** - to have the Switch send information to the accounting server only when a user ends a session.
Method	Select whether you want to use RADIUS or TACACS+ for accounting of specific types of events. TACACS+ is the only method for recording **Commands** type of event.
Privilege	This field is only configurable for **Commands** type of event. Select the threshold command privilege level for which the Switch should send accounting information. The Switch will send accounting information when commands at the level you specify and higher are executed on the Switch.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23.2.4 Vendor Specific Attribute

RFC 2865 standard specifies a method for sending vendor-specific information between a RADIUS server and a network access device (for example, the Switch). A company can create Vendor Specific Attributes (VSAs) to expand the functionality of a RADIUS server.

The Switch supports VSAs that allow you to perform the following actions based on user authentication:

- Limit bandwidth on incoming or outgoing traffic for the port the user connects to.
- Assign account privilege levels (see the CLI Reference Guide for more information on account privilege levels) for the authenticated user.

The VSAs are composed of the following:

- **Vendor-ID**: An identification number assigned to the company by the IANA (Internet Assigned Numbers Authority). ZyXEL's vendor ID is 890.
- **Vendor-Type**: A vendor specified attribute, identifying the setting you want to modify.
- **Vendor-data**: A value you want to assign to the setting.

Note: Refer to the documentation that comes with your RADIUS server on how to configure VSAs for users authenticating via the RADIUS server.

The following table describes the VSAs supported on the Switch. Note that these attributes only work when you enable authorization (see Section 23.2.3 on page 193).

Table 77 Supported VSAs

FUNCTION	ATTRIBUTE
Ingress Bandwidth Assignment	Vendor-Id = **890** Vendor-Type = **1** Vendor-data = ingress rate (Kbps in decimal format)
Egress Bandwidth Assignment	Vendor-Id = **890** Vendor-Type = **2** Vendor-data = egress rate (Kbps in decimal format)
Privilege Assignment	Vendor-ID = **890** Vendor-Type = **3** Vendor-Data = "**shell:priv-lvl=**N" or Vendor-ID = **9** (CISCO) Vendor-Type = **1** (CISCO-AVPAIR) Vendor-Data = "**shell:priv-lvl=**N" where N is a privilege level (from 0 to 14). Note: If you set the privilege level of a login account differently on the RADIUS server(s) and the Switch, the user is assigned a privilege level from the database (RADIUS or local) the Switch uses first for user authentication.

23.2.5 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server (refer to your RADIUS server documentation) to assign a port on the Switch to a VLAN based on IEEE 802.1x authentication. The port VLAN settings are fixed and untagged. This will also set the port's VID. The following table describes the values you need to configure. Note that these attributes only work when you enable authorization (see Section 23.2.3 on page 193).

Table 78 Supported Tunnel Protocol Attribute

FUNCTION	ATTRIBUTE
VLAN Assignment	Tunnel-Type = **VLAN(13)** Tunnel-Medium-Type = **802(6)** Tunnel-Private-Group-ID = VLAN ID Note: You must also create a VLAN with the specified VID on the Switch. Note: The bolded values in this table are fixed values as defined in RFC 3580.

23.3 Supported RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are data used to define specific authentication, and accounting elements in a user profile, which is stored on the RADIUS server. This section lists the RADIUS attributes supported by the Switch.

Refer to RFC 2865 for more information about RADIUS attributes used for authentication. Refer to RFC 2866 and RFC 2869 for RADIUS attributes used for accounting.

This section lists the attributes used by authentication and accounting functions on the Switch. In cases where the attribute has a specific format associated with it, the format is specified.

23.3.1 Attributes Used for Authentication

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

23.3.1.1 Attributes Used for Authenticating Privilege Access

User-Name
- the format of the User-Name attribute is **$enab#$**, where # is the privilege level (1-14)

User-Password

NAS-Identifier

NAS-IP-Address

23.3.1.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

23.3.1.3 Attributes Used by the IEEE 802.1x Authentication

User-Name

NAS-Identifier

NAS-IP-Address

NAS-Port

NAS-Port-Type
- This value is set to **Ethernet(15)** on the Switch.

Calling-Station-Id

Frame-MTU

EAP-Message

State

Message-Authenticator

23.3.2 Attributes Used for Accounting

The following sections list the attributes sent from the Switch to the RADIUS server when performing authentication.

23.3.2.1 Attributes Used for Accounting System Events

NAS-IP-Address

NAS-Identifier

Acct-Status-Type

Acct-Session-ID
- The format of Acct-Session-Id is **date+time+8-digit sequential number**, for example, 200704191721030000000001. (date: 2007/04/19, time: 17:21:03, serial number: 00000001)

Acct-Delay-Time

23.3.2.2 Attributes Used for Accounting Exec Events

The attributes are listed in the following table along with the time that they are sent (the difference between Console and Telnet/SSH Exec events is that the Telnet/SSH events utilize the Calling-Station-Id attribute):

Table 79 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	✔	✔	✔
NAS-Identifier	✔	✔	✔
NAS-IP-Address	✔	✔	✔
Service-Type	✔	✔	✔
Acct-Status-Type	✔	✔	✔
Acct-Delay-Time	✔	✔	✔
Acct-Session-Id	✔	✔	✔
Acct-Authentic	✔	✔	✔
Acct-Session-Time		✔	✔
Acct-Terminate-Cause			✔

Table 80 RADIUS Attributes - Exec Events via Telnet/SSH

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	✔	✔	✔
NAS-Identifier	✔	✔	✔
NAS-IP-Address	✔	✔	✔
Service-Type	✔	✔	✔
Calling-Station-Id	✔	✔	✔
Acct-Status-Type	✔	✔	✔
Acct-Delay-Time	✔	✔	✔
Acct-Session-Id	✔	✔	✔
Acct-Authentic	✔	✔	✔
Acct-Session-Time		✔	✔
Acct-Terminate-Cause			✔

23.3.2.3 Attributes Used for Accounting IEEE 802.1x Events

The attributes are listed in the following table along with the time of the session they are sent:

Table 81 RADIUS Attributes - Exec Events via Console

ATTRIBUTE	START	INTERIM-UPDATE	STOP
User-Name	✔	✔	✔
NAS-IP-Address	✔	✔	✔
NAS-Port	✔	✔	✔
Class	✔	✔	✔
Called-Station-Id	✔	✔	✔
Calling-Station-Id	✔	✔	✔
NAS-Identifier	✔	✔	✔
NAS-Port-Type	✔	✔	✔
Acct-Status-Type	✔	✔	✔
Acct-Delay-Time	✔	✔	✔
Acct-Session-Id	✔	✔	✔
Acct-Authentic	✔	✔	✔
Acct-Input-Octets		✔	✔
Acct-Output-Octets		✔	✔
Acct-Session-Time		✔	✔
Acct-Input-Packets		✔	✔
Acct-Output-Packets		✔	✔
Acct-Terminate-Cause			✔
Acct-Input-Gigawords		✔	✔
Acct-Output-Gigawords		✔	✔

24

IP Source Guard

Use IP source guard to filter unauthorized DHCP and ARP packets in your network.

24.1 IP Source Guard Overview

IP source guard uses a binding table to distinguish between authorized and unauthorized DHCP and ARP packets in your network. A binding contains these key attributes:

- MAC address
- VLAN ID
- IP address
- Port number

When the Switch receives a DHCP or ARP packet, it looks up the appropriate MAC address, VLAN ID, IP address, and port number in the binding table. If there is a binding, the Switch forwards the packet. If there is not a binding, the Switch discards the packet.

The Switch builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

IP source guard consists of the following features:

- Static bindings. Use this to create static bindings in the binding table.
- DHCP snooping. Use this to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.

If you want to use dynamic bindings to filter unauthorized ARP packets (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

24.1.1 IP Source Guard Menu Overview

Table 82 IP Source Guard Menu Overview

MENU	SUB-MENU 1	SUB-MENU 2	SUB-MENU 3
IP Source Guard	Static Binding		
	DHCP Snooping	Configure	Port
			VLAN
	ARP Inspection	VLAN Status	
		Log Status	
		Configure	Port
			VLAN

24.1.2 DHCP Snooping Overview

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

24.1.2.1 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted/untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the packet do not match any of the current bindings.
- The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP packets arrive is too high.

24.1.2.2 DHCP Snooping Database

The Switch stores the binding table in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again. As a result, it is recommended you configure the DHCP snooping database.

The DHCP snooping database maintains the dynamic bindings for DHCP snooping and ARP inspection in a file on an external TFTP server. If you set up the DHCP snooping database, the Switch can reload the dynamic bindings from the DHCP snooping database after the Switch restarts.

You can configure the name and location of the file on the external TFTP server. The file has the following format:

Figure 106 DHCP Snooping Database File Format

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<binding-1> <checksum-1>
<binding-2> <checksum-1-2>
...
...
<binding-n> <checksum-1-2-..-n>
END
```

The <initial-checksum> helps distinguish between the bindings in the latest update and the bindings from previous updates. Each binding consists of 72 bytes, a space, and another checksum that is used to validate the binding when it is read. If the calculated checksum is not equal to the checksum in the file, that binding and all others after it are ignored.

24.1.2.3 DHCP Relay Option 82 Information

The Switch can add information to DHCP requests that it does not discard. This provides the DHCP server more information about the source of the requests. The Switch can add the following information:

- Slot ID (1 byte), port ID (1 byte), and source VLAN ID (2 bytes)
- System name (up to 32 bytes)

This information is stored in an Agent Information field in the option 82 field of the DHCP headers of client DHCP request frames. See Chapter 34 on page 263 for more information about DHCP relay option 82.

When the DHCP server responds, the Switch removes the information in the Agent Information field before forwarding the response to the original source.

You can configure this setting for each source VLAN. This setting is independent of the DHCP relay settings (Chapter 34 on page 263).

24.1.2.4 Configuring DHCP Snooping

Follow these steps to configure DHCP snooping on the Switch.

1. Enable DHCP snooping on the Switch.
2. Enable DHCP snooping on each VLAN, and configure DHCP relay option 82.

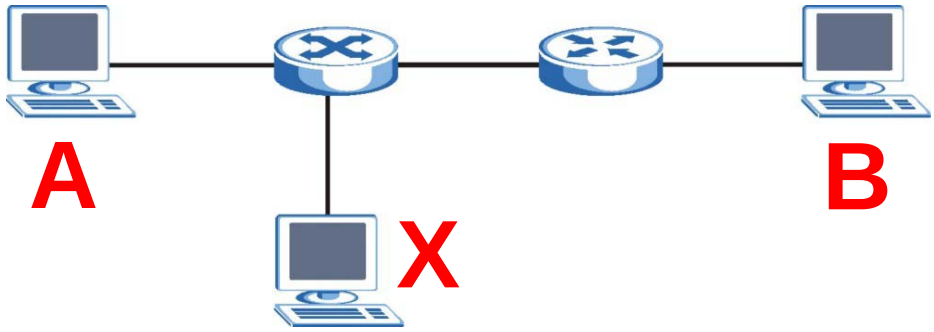
3 Configure trusted and untrusted ports, and specify the maximum number of DHCP packets that each port can receive per second.

4 Configure static bindings.

24.1.3 ARP Inspection Overview

Use ARP inspection to filter unauthorized ARP packets on the network. This can prevent many kinds of man-in-the-middle attacks, such as the one in the following example.

Figure 107 Example: Man-in-the-middle Attack



In this example, computer **B** tries to establish a connection with computer **A**. Computer **X** is in the same broadcast domain as computer **A** and intercepts the ARP request for computer **A**. Then, computer **X** does the following things:

- It pretends to be computer **A** and responds to computer **B**.
- It pretends to be computer **B** and sends a message to computer **A**.

As a result, all the communication between computer **A** and computer **B** passes through computer **X**. Computer **X** can read and alter the information passed between them.

24.1.3.1 ARP Inspection and MAC Address Filters

When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. You can configure how long the MAC address filter remains in the Switch.

These MAC address filters are different than regular MAC address filters (Chapter 10 on page 105).

- They are stored only in volatile memory.
- They do not use the same space in memory that regular MAC address filters use.
- They appear only in the **ARP Inspection** screens and commands, not in the **MAC Address Filter** screens and commands.

24.1.3.2 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for ARP inspection. This setting is independent of the trusted/untrusted setting for DHCP snooping. You can also specify the maximum rate at which the Switch receives ARP packets on untrusted ports.

The Switch does not discard ARP packets on trusted ports for any reason.

The Switch discards ARP packets on untrusted ports in the following situations:

- The sender's information in the ARP packet does not match any of the current bindings.
- The rate at which ARP packets arrive is too high.

24.1.3.3 Syslog

The Switch can send syslog messages to the specified syslog server (Chapter 38 on page 297) when it forwards or discards ARP packets. The Switch can consolidate log messages and send log messages in batches to make this mechanism more efficient.

24.1.3.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

1. Configure DHCP snooping. See Section 24.1.2.4 on page 202.

   Note: It is recommended you enable DHCP snooping at least one day before you enable ARP inspection so that the Switch has enough time to build the binding table.

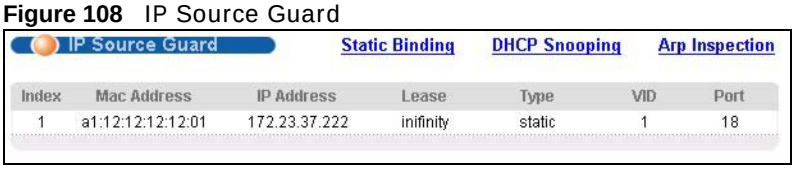
2. Enable ARP inspection on each VLAN.

3. Configure trusted and untrusted ports, and specify the maximum number of ARP packets that each port can receive per second.

24.2 IP Source Guard

Use this screen to look at the current bindings for DHCP snooping and ARP inspection. Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized packets in the network. The Switch learns the bindings by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings). To open this screen, click **Advanced Application > IP Source Guard**.

Figure 108 IP Source Guard



The following table describes the labels in this screen.

Table 83 IP Source Guard

LABEL	DESCRIPTION
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how many days, hours, minutes, and seconds the binding is valid; for example, **2d3h4m5s** means the binding is still valid for 2 days, 3 hours, 4 minutes and 5 seconds. This field displays **infinity** if the binding is always valid (for example, a static binding).

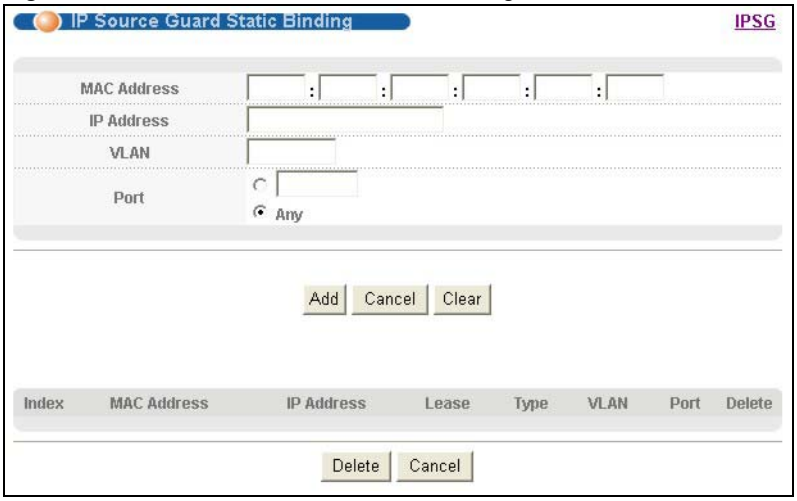
Table 83 IP Source Guard (continued)

LABEL	DESCRIPTION
Type	This field displays how the Switch learned the binding. **static**: This binding was learned from information provided manually by an administrator. **dhcp-snooping**: This binding was learned by snooping DHCP packets.
VID	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.

24.3 Static Binding

Use this screen to manage static bindings for DHCP snooping and ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the new static binding replaces the original one. To open this screen, click **Advanced Application > IP Source Guard > Static Binding**.

Figure 109 IP Source Guard Static Binding



The following table describes the labels in this screen.

Table 84 IP Source Guard Static Binding

LABEL	DESCRIPTION
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN	Enter the source VLAN ID in the binding.
Port	Specify the port(s) in the binding. If this binding has one port, select the first radio button and enter the port number in the field to the right. If this binding applies to all ports, select **Any**.
Add	Click this to create the specified static binding or to update an existing one.
Cancel	Click this to reset the values above based on the last selected static binding or, if not applicable, to clear the fields above.

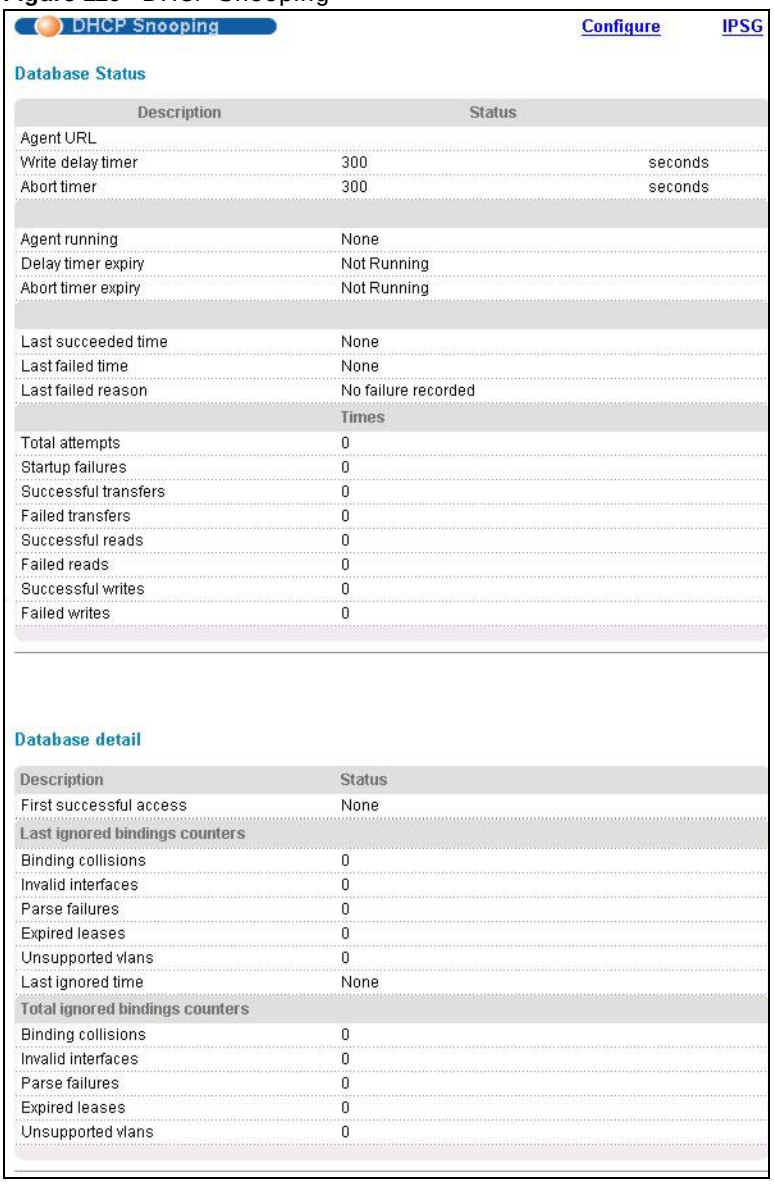
Table 84 IP Source Guard Static Binding (continued)

LABEL	DESCRIPTION
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays a sequential number for each binding.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how long the binding is valid.
Type	This field displays how the Switch learned the binding. **static**: This binding was learned from information provided manually by an administrator.
VLAN	This field displays the source VLAN ID in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.
Delete	Select this, and click **Delete** to remove the specified entry.
Cancel	Click this to clear the **Delete** check boxes above.

24.4 DHCP Snooping

Use this screen to look at various statistics about the DHCP snooping database. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping**.

Figure 110 DHCP Snooping



The following table describes the labels in this screen.

Table 85 DHCP Snooping

LABEL	DESCRIPTION
Database Status	
	This section displays the current settings for the DHCP snooping database. You can configure them in the **DHCP Snooping Configure** screen. See Section 24.5 on page 209.
Agent URL	This field displays the location of the DHCP snooping database.

Table 85 DHCP Snooping (continued)

LABEL	DESCRIPTION
Write delay timer	This field displays how long (in seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Abort timer	This field displays how long (in seconds) the Switch waits to update the DHCP snooping database after the current bindings change.
	This section displays information about the current update and the next update of the DHCP snooping database.
Agent running	This field displays the status of the current update or access of the DHCP snooping database. **none**: The Switch is not accessing the DHCP snooping database. **read**: The Switch is loading dynamic bindings from the DHCP snooping database. **write**: The Switch is updating the DHCP snooping database.
Delay timer expiry	This field displays how much longer (in seconds) the Switch tries to complete the current update before it gives up. It displays **Not Running** if the Switch is not updating the DHCP snooping database right now.
Abort timer expiry	This field displays when (in seconds) the Switch is going to update the DHCP snooping database again. It displays **Not Running** if the current bindings have not changed since the last update.
	This section displays information about the last time the Switch updated the DHCP snooping database.
Last succeeded time	This field displays the last time the Switch updated the DHCP snooping database successfully.
Last failed time	This field displays the last time the Switch updated the DHCP snooping database unsuccessfully.
Last failed reason	This field displays the reason the Switch updated the DHCP snooping database unsuccessfully.
	This section displays historical information about the number of times the Switch successfully or unsuccessfully read or updated the DHCP snooping database.
Total attempts	This field displays the number of times the Switch has tried to access the DHCP snooping database for any reason.
Startup failures	This field displays the number of times the Switch could not create or read the DHCP snooping database when the Switch started up or a new URL is configured for the DHCP snooping database.
Successful transfers	This field displays the number of times the Switch read bindings from or updated the bindings in the DHCP snooping database successfully.
Failed transfers	This field displays the number of times the Switch was unable to read bindings from or update the bindings in the DHCP snooping database.
Successful reads	This field displays the number of times the Switch read bindings from the DHCP snooping database successfully.
Failed reads	This field displays the number of times the Switch was unable to read bindings from the DHCP snooping database.
Successful writes	This field displays the number of times the Switch updated the bindings in the DHCP snooping database successfully.
Failed writes	This field displays the number of times the Switch was unable to update the bindings in the DHCP snooping database.
Database detail	
First successful access	This field displays the first time the Switch accessed the DHCP snooping database for any reason.

Table 85 DHCP Snooping (continued)

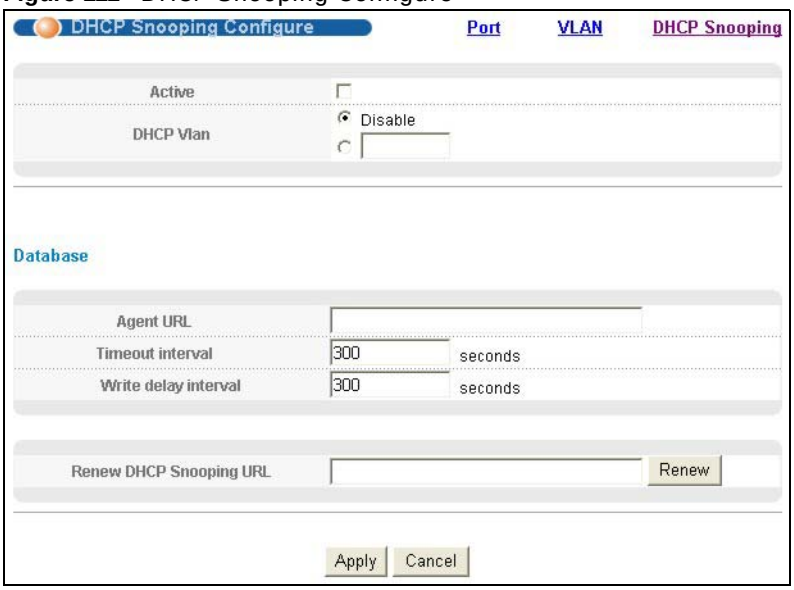
LABEL	DESCRIPTION
Last ignored bindings counters	This section displays the number of times and the reasons the Switch ignored bindings the last time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch or using CLI commands. See the Ethernet Switch CLI Reference Guide.
Binding collisions	This field displays the number of bindings the Switch ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the Switch ignored because the port number was a trusted interface or does not exist anymore.
Parse failures	This field displays the number of bindings the Switch ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch ignored because the VLAN ID does not exist anymore.
Last ignored time	This field displays the last time the Switch ignored any bindings for any reason from the DHCP binding database.
Total ignored bindings counters	This section displays the reasons the Switch has ignored bindings any time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch or using CLI commands. See the Ethernet Switch CLI Reference Guide.
Binding collisions	This field displays the number of bindings the Switch has ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the Switch has ignored because the port number was a trusted interface or does not exist anymore.
Parse failures	This field displays the number of bindings the Switch has ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch has ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch has ignored because the VLAN ID does not exist anymore.

24.5 DHCP Snooping Configure

Use this screen to enable DHCP snooping on the Switch (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database. The DHCP snooping database stores the current bindings on a secure, external TFTP server so that they are

still available after a restart. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure**.

Figure 111 DHCP Snooping Configure



The following table describes the labels in this screen.

Table 86 DHCP Snooping Configure

LABEL	DESCRIPTION
Active	Select this to enable DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLAN and specify trusted ports. Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.
DHCP Vlan	Select a VLAN ID if you want the Switch to forward DHCP packets to DHCP servers on a specific VLAN. Note: You have to enable DHCP snooping on the DHCP VLAN too. You can enable **Option82** in the **DHCP Snooping VLAN Configure** screen (Section 24.5.2 on page 212) to help the DHCP servers distinguish between DHCP requests from different VLAN. Select **Disable** if you do not want the Switch to forward DHCP packets to a specific VLAN.
Database	If **Timeout interval** is greater than **Write delay interval**, it is possible that the next update is scheduled to occur before the current update has finished successfully or timed out. In this case, the Switch waits to start the next update until it completes the current one.
Agent URL	Enter the location of the DHCP snooping database. The location should be expressed like this: **tftp://{domain name or IP address}/directory, if applicable/file name**; for example, **tftp://192.168.10.1/database.txt.**
Timeout interval	Enter how long (10-65535 seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Write delay interval	Enter how long (10-65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update. Once the next update is scheduled, additional changes in current bindings are automatically included in the next update.

Table 86 DHCP Snooping Configure (continued)

LABEL	DESCRIPTION
Renew DHCP Snooping URL	Enter the location of a DHCP snooping database, and click **Renew** if you want the Switch to load it. You can use this to load dynamic bindings from a different DHCP snooping database than the one specified in **Agent URL**. When the Switch loads dynamic bindings from a DHCP snooping database, it does not discard the current dynamic bindings first. If there is a conflict, the Switch keeps the dynamic binding in volatile memory and updates the **Binding collisions** counter in the **DHCP Snooping** screen (Section 24.4 on page 207).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

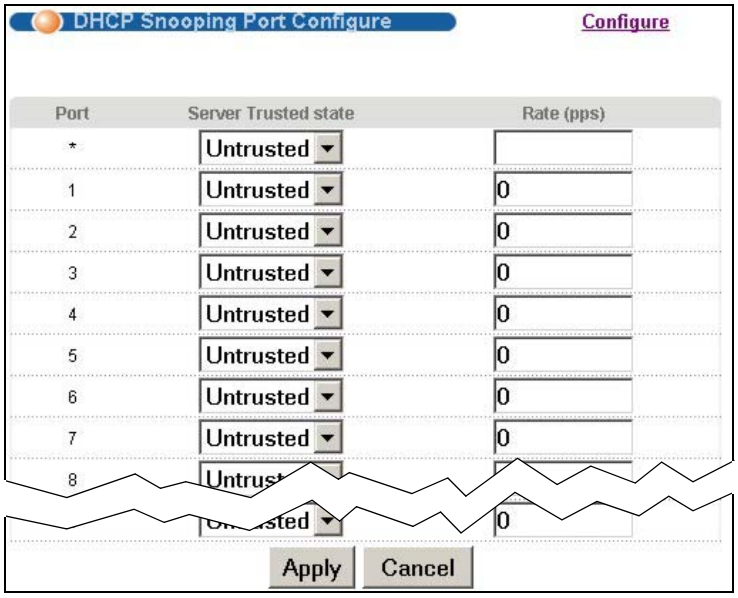
24.5.1 DHCP Snooping Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for DHCP snooping.

Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.

You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > Port**.

Figure 112 DHCP Snooping Port Configure



The following table describes the labels in this screen.

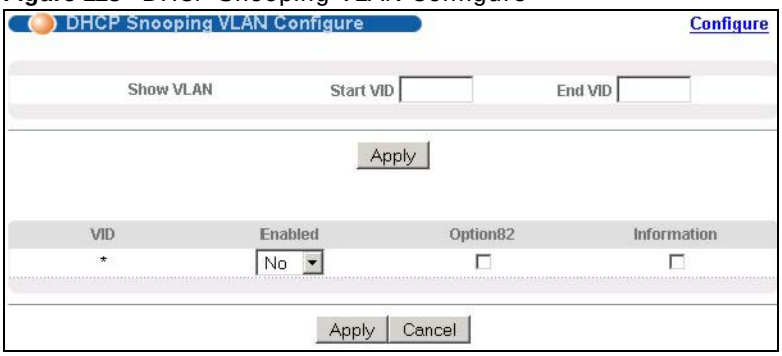
Table 87 DHCP Snooping Port Configure

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
Server Trusted state	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). Trusted ports are connected to DHCP servers or other switches, and the Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. Untrusted ports are connected to subscribers, and the Switch discards DHCP packets from untrusted ports in the following situations: • The packet is a DHCP server packet (for example, OFFER, ACK, or NACK). • The source MAC address and source IP address in the packet do not match any of the current bindings. • The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings. • The rate at which DHCP packets arrive is too high.
Rate (pps)	Specify the maximum number for DHCP packets (1-2048) that the Switch receives from each port each second. The Switch discards any additional DHCP packets. Enter 0 to disable this limit, which is recommended for trusted ports.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

24.5.2 DHCP Snooping VLAN Configure

Use this screen to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information (Chapter 34 on page 263) to DHCP requests that the Switch relays to a DHCP server for each VLAN. To open this screen, click **Advanced Application > IP Source Guard > DHCP Snooping > Configure > VLAN**.

Figure 113 DHCP Snooping VLAN Configure



The following table describes the labels in this screen.

Table 88 DHCP Snooping VLAN Configure

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.

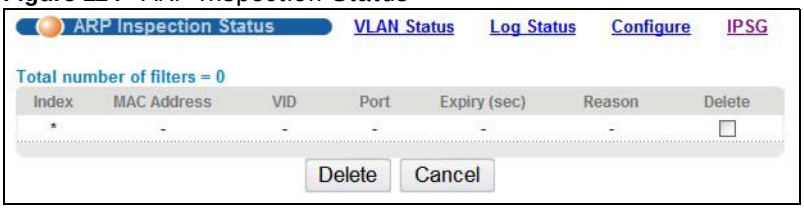
Table 88 DHCP Snooping VLAN Configure (continued)

LABEL	DESCRIPTION
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
Enabled	Select **Yes** to enable DHCP snooping on the VLAN. You still have to enable DHCP snooping on the Switch and specify trusted ports. Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.
Option82	Select this to have the Switch add the slot number, port number and VLAN ID to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the **DHCP Snooping Configure** screen. See Section 24.5 on page 209.
Information	Select this to have the Switch add the system name to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can configure the system name in the **General Setup** screen. See Chapter 6 on page 70. You can specify the DHCP VLAN in the **DHCP Snooping Configure** screen. See Section 24.5 on page 209.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

24.6 ARP Inspection

Use this screen to look at the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection**.

Figure 114 ARP Inspection Status



The following table describes the labels in this screen.

Table 89 ARP Inspection Status

LABEL	DESCRIPTION
Total number of filters	This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.
Index	This field displays a sequential number for each MAC address filter.
MAC Address	This field displays the source MAC address in the MAC address filter.
VID	This field displays the source VLAN ID in the MAC address filter.

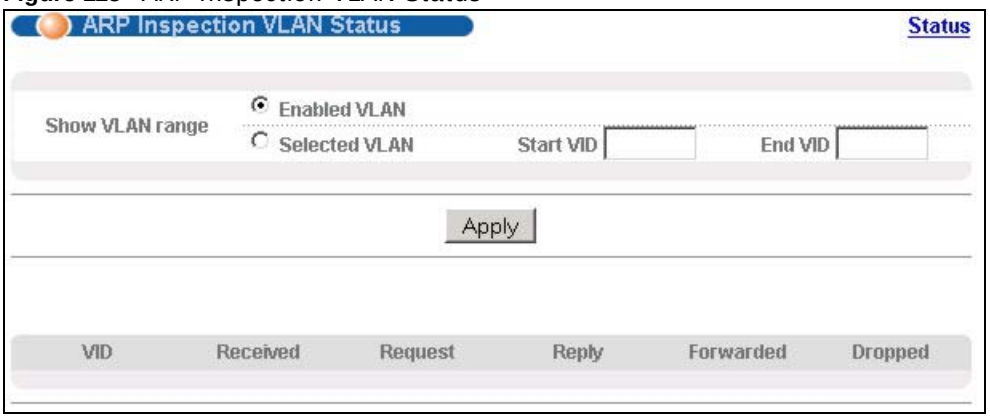
Table 89 ARP Inspection Status (continued)

LABEL	DESCRIPTION
Port	This field displays the source port of the discarded ARP packet.
Expiry (sec)	This field displays how long (in seconds) the MAC address filter remains in the Switch. You can also delete the record manually (**Delete**).
Reason	This field displays the reason the ARP packet was discarded. **MAC+VLAN**: The MAC address and VLAN ID were not in the binding table. **IP**: The MAC address and VLAN ID were in the binding table, but the IP address was not valid. **Port**: The MAC address, VLAN ID, and IP address were in the binding table, but the port number was not valid.
Delete	Select this and click **Delete** to remove the specified entry.
Delete	Click this to remove the selected entries.
Cancel	Click this to clear the **Delete** check boxes above.

24.6.1 ARP Inspection VLAN Status

Use this screen to look at various statistics about ARP packets in each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > VLAN Status**.

Figure 115 ARP Inspection VLAN Status



The following table describes the labels in this screen.

Table 90 ARP Inspection VLAN Status

LABEL	DESCRIPTION
Show VLAN range	Use this section to specify the VLANs you want to look at in the section below.
Enabled VLAN	Select this to look at all the VLANs on which ARP inspection is enabled in the section below.
Selected VLAN	Select this to look at all the VLANs in a specific range in the section below. Then, enter the lowest VLAN ID (**Start VID**) and the highest VLAN ID (**End VID**) you want to look at.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above.
Received	This field displays the total number of ARP packets received from the VLAN since the Switch last restarted.

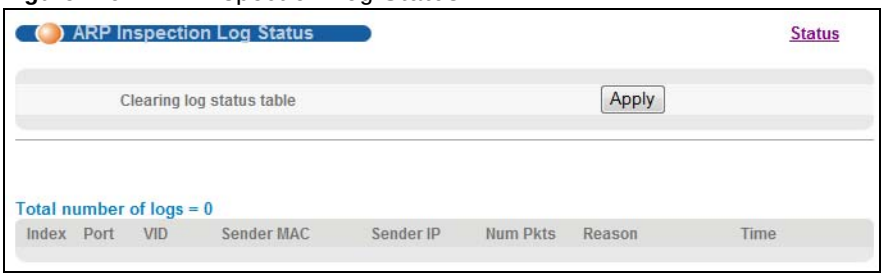
Table 90 ARP Inspection VLAN Status

LABEL	DESCRIPTION
Request	This field displays the total number of ARP Request packets received from the VLAN since the Switch last restarted.
Reply	This field displays the total number of ARP Reply packets received from the VLAN since the Switch last restarted.
Forwarded	This field displays the total number of ARP packets the Switch forwarded for the VLAN since the Switch last restarted.
Dropped	This field displays the total number of ARP packets the Switch discarded for the VLAN since the Switch last restarted.

24.6.2 ARP Inspection Log Status

Use this screen to look at log messages that were generated by ARP packets and that have not been sent to the syslog server yet. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Log Status**.

Figure 116 ARP Inspection Log Status



The following table describes the labels in this screen.

Table 91 ARP Inspection Log Status

LABEL	DESCRIPTION
Clearing log status table	Click **Apply** to remove all the log messages that were generated by ARP packets and that have not been sent to the syslog server yet.
Total number of logs	This field displays the number of log messages that were generated by ARP packets and that have not been sent to the syslog server yet. If one or more log messages are dropped due to unavailable buffer, there is an entry called **overflow** with the current number of dropped log messages.
Index	This field displays a sequential number for each log message.
Port	This field displays the source port of the ARP packet.
VID	This field displays the source VLAN ID of the ARP packet.
Sender MAC	This field displays the source MAC address of the ARP packet.
Sender IP	This field displays the source IP address of the ARP packet.
Num Pkts	This field displays the number of ARP packets that were consolidated into this log message. The Switch consolidates identical log messages generated by ARP packets in the log consolidation interval into one log message. You can configure this interval in the **ARP Inspection Configure** screen. See Section 24.7 on page 216.

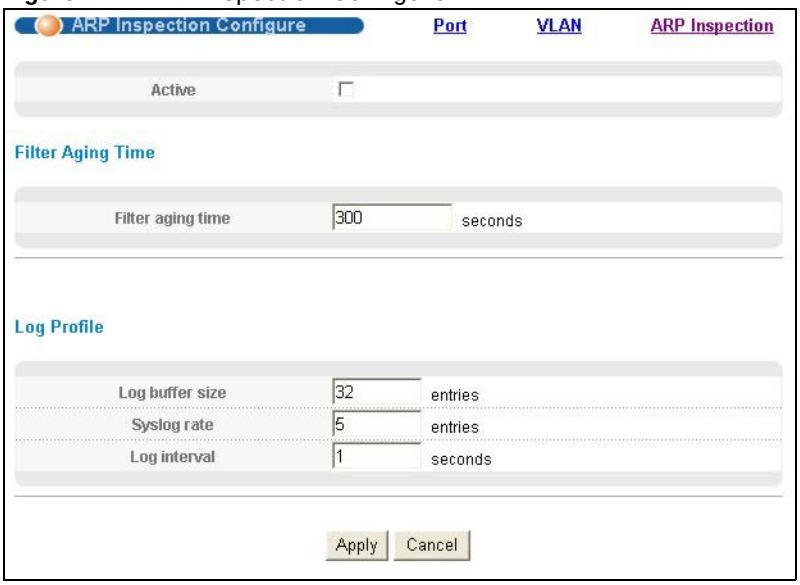
Table 91 ARP Inspection Log Status (continued)

LABEL	DESCRIPTION
Reason	This field displays the reason the log message was generated. **dhcp deny**: An ARP packet was discarded because it violated a dynamic binding with the same MAC address and VLAN ID. **static deny**: An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID. **deny**: An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID. **dhcp permit**: An ARP packet was forwarded because it matched a dynamic binding. **static permit**: An ARP packet was forwarded because it matched a static binding. In the **ARP Inspection VLAN Configure** screen, you can configure the Switch to generate log messages when ARP packets are discarded or forwarded based on the VLAN ID of the ARP packet. See Section 24.7.2 on page 219.
Time	This field displays when the log message was generated.

24.7 ARP Inspection Configure

Use this screen to enable ARP inspection on the Switch. You can also configure the length of time the Switch stores records of discarded ARP packets and global settings for the ARP inspection log. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure**.

Figure 117 ARP Inspection Configure



The following table describes the labels in this screen.

Table 92 ARP Inspection Configure

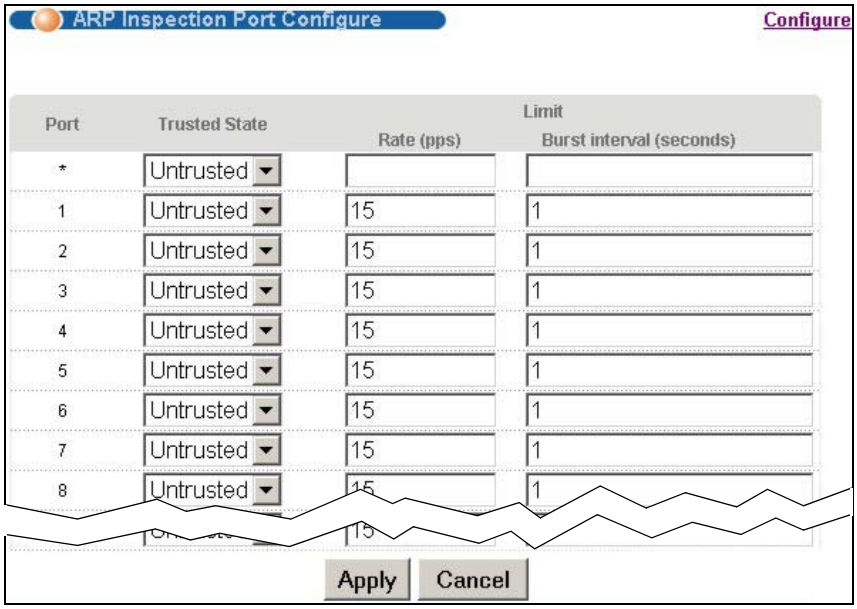
LABEL	DESCRIPTION
Active	Select this to enable ARP inspection on the Switch. You still have to enable ARP inspection on specific VLAN and specify trusted ports.
Filter Aging Time	
Filter aging time	This setting has no effect on existing MAC address filters. Enter how long (1-2147483647 seconds) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards. Type 0 if you want the MAC address filter to be permanent.
Log Profile	
Log buffer size	Enter the maximum number (1-1024) of log messages that were generated by ARP packets and have not been sent to the syslog server yet. Make sure this number is appropriate for the specified **Syslog rate** and **Log interval**. If the number of log messages in the Switch exceeds this number, the Switch stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer. Click **Clearing log status table** in the **ARP Inspection Log Status** screen to clear the log and reset this counter. See Section 24.6.2 on page 215.
Syslog rate	Type the maximum number of syslog messages the Switch can send to the syslog server in one batch. This number is expressed as a rate because the batch frequency is determined by the **Log Interval**. You must configure the syslog server (Chapter 38 on page 297) to use this. Enter 0 if you do not want the Switch to send log messages generated by ARP packets to the syslog server. The relationship between **Syslog rate** and **Log interval** is illustrated in the following examples: • 4 invalid ARP packets per second, **Syslog rate** is 5, **Log interval** is 1: the Switch sends 4 syslog messages every second. • 6 invalid ARP packets per second, **Syslog rate** is 5, **Log interval** is 2: the Switch sends 5 syslog messages every 2 seconds.
Log interval	Type how often (1-86400 seconds) the Switch sends a batch of syslog messages to the syslog server. Enter 0 if you want the Switch to send syslog messages immediately. See **Syslog rate** for an example of the relationship between **Syslog rate** and **Log interval**.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

24.7.1 ARP Inspection Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for ARP inspection. You can also specify the maximum rate at which the Switch receives ARP packets on each untrusted port. To

open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > Port**.

Figure 118 ARP Inspection Port Configure



The following table describes the labels in this screen.

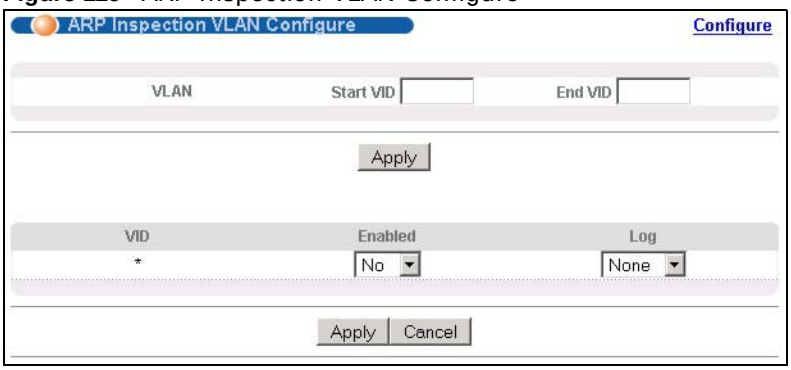
Table 93 ARP Inspection Port Configure

LABEL	DESCRIPTION
Port	This field displays the port number. If you configure the ***** port, the settings are applied to all of the ports.
Trusted State	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports in the following situations: • The sender's information in the ARP packet does not match any of the current bindings. • The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on untrusted ports.
Limit	Rate and Burst Interval settings have no effect on trusted ports.
Rate (pps)	Specify the maximum rate (1-2048 packets per second) at which the Switch receives ARP packets from each port. The Switch discards any additional ARP packets. Enter 0 to disable this limit.
Burst interval (seconds)	The burst interval is the length of time over which the rate of ARP packets is monitored for each port. For example, if the Rate is 15 pps and the burst interval is 1 second, then the Switch accepts a maximum of 15 ARP packets in every one-second interval. If the burst interval is 5 seconds, then the Switch accepts a maximum of 75 ARP packets in every five-second interval. Enter the length (1-15 seconds) of the burst interval.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

24.7.2 ARP Inspection VLAN Configure

Use this screen to enable ARP inspection on each VLAN and to specify when the Switch generates log messages for receiving ARP packets from each VLAN. To open this screen, click **Advanced Application > IP Source Guard > ARP Inspection > Configure > VLAN**.

Figure 119 ARP Inspection VLAN Configure



The following table describes the labels in this screen.

Table 94 ARP Inspection VLAN Configure

LABEL	DESCRIPTION
VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
Enabled	Select **Yes** to enable ARP inspection on the VLAN. Select **No** to disable ARP inspection on the VLAN.
Log	Specify when the Switch generates log messages for receiving ARP packets from the VLAN. **None**: The Switch does not generate any log messages when it receives an ARP packet from the VLAN. **Deny**: The Switch generates log messages when it discards an ARP packet from the VLAN. **Permit**: The Switch generates log messages when it forwards an ARP packet from the VLAN. **All**: The Switch generates log messages every time it receives an ARP packet from the VLAN.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

25

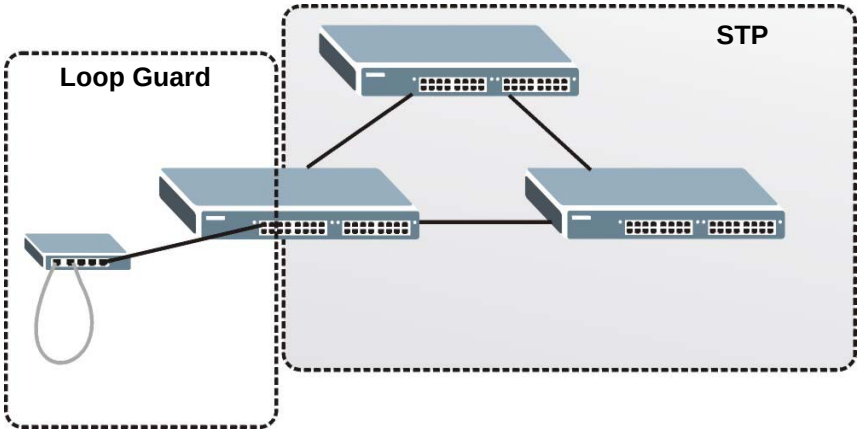
Loop Guard

This chapter shows you how to configure the Switch to guard against loops on the edge of your network.

25.1 Loop Guard Overview

Loop guard allows you to configure the Switch to shut down a port if it detects that packets sent out on that port loop back to the Switch. While you can use Spanning Tree Protocol (STP) to prevent loops in the core of your network. STP cannot prevent loops that occur on the edge of your network.

Figure 120 Loop Guard vs STP



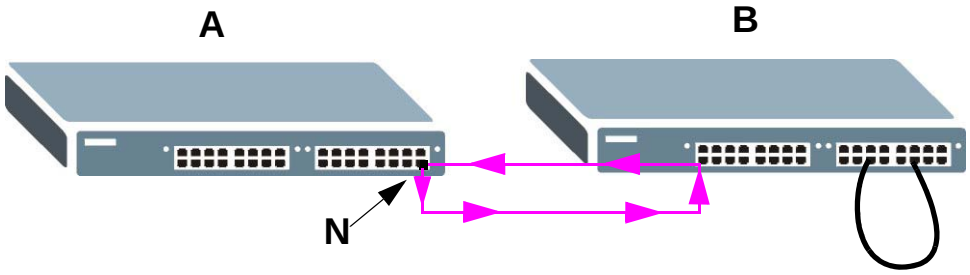
Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on switch **A** connected to switch **B**. Switch **B** is in loop state. When broadcast or multicast packets leave port **N** and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from **B**.

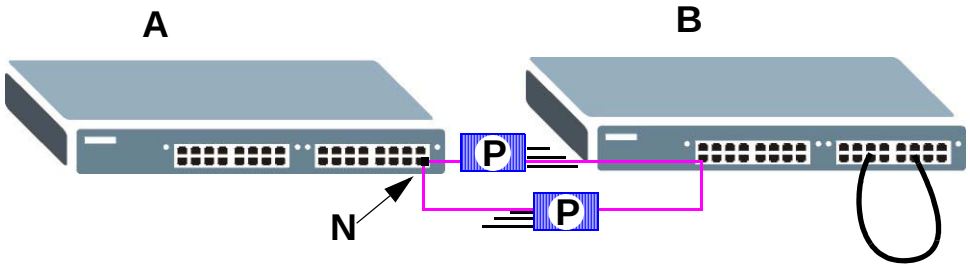
Figure 121 Switch in Loop State



The loop guard feature checks to see if a loop guard enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop state.

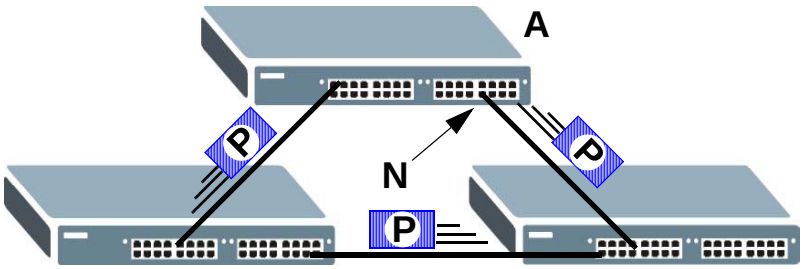
The following figure shows a loop guard enabled port **N** on switch **A** sending a probe packet **P** to switch **B**. Since switch **B** is in loop state, the probe packet **P** returns to port **N** on **A**. The Switch then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

Figure 122 Loop Guard - Probe Packet



The Switch also shuts down port **N** if the probe packet returns to switch **A** on any other port. In other words loop guard also protects against standard network loops. The following figure illustrates three switches forming a loop. A sample path of the loop guard probe packet is also shown. In this example, the probe packet is sent from port **N** and returns on another port. As long as loop guard is enabled on port **N**. The Switch will shut down port **N** if it detects that the probe packet has returned to the Switch.

Figure 123 Loop Guard - Network Loop



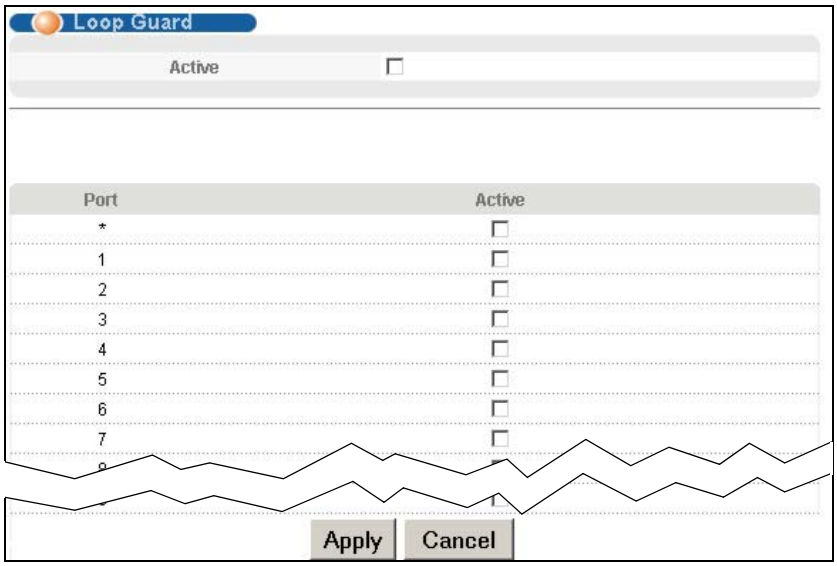
Note: After resolving the loop problem on your network you can re-activate the disabled port via the web configurator (see Section 6.7 on page 78) or via commands (see the Ethernet Switch CLI Reference Guide).

25.2 Loop Guard Setup

Click **Advanced Application** > **Loop Guard** in the navigation panel to display the screen as shown.

Note: The loop guard feature can not be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.

Figure 124 Advanced Application > Loop Guard



The following table describes the labels in this screen.

Table 95 Advanced Application > Loop Guard

LABEL	DESCRIPTION
Active	Select this option to enable loop guard on the Switch. The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop guard feature.
Port	This field displays a port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the loop guard feature on this port. The Switch sends probe packets from this port to check if the Switch it is connected to is in loop state. If the Switch that this port is connected is in loop state the Switch will shut down this port. Clear this check box to disable the loop guard feature.

Table 95 Advanced Application > Loop Guard (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

26

VLAN Mapping

This chapter shows you how to configure VLAN mapping on the Switch.

26.1 VLAN Mapping Overview

With VLAN mapping enabled, the Switch can map the VLAN ID and priority level of packets received from a private network to those used in the service provider's network.

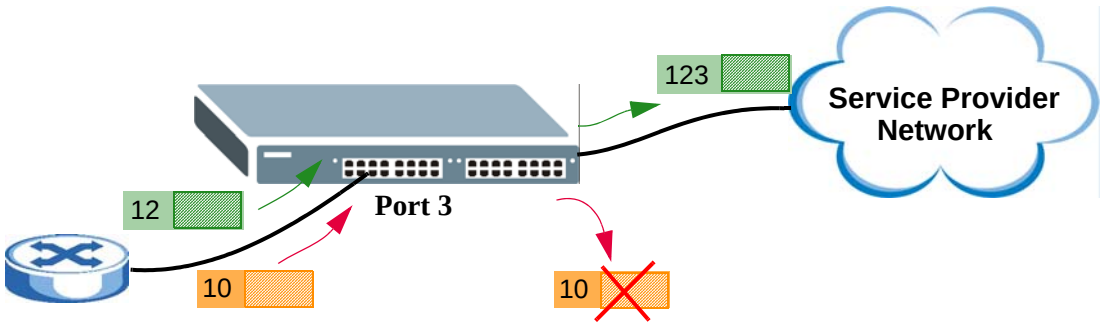
The Switch checks incoming traffic from the switch ports (non-management ports) against the VLAN mapping table first, the MAC learning table and then the VLAN table before forwarding them through the Gigabit uplink port. When VLAN mapping is enabled, the Switch discards the tagged packets that do not match an entry in the VLAN mapping table. If the incoming packets are untagged, the Switch adds a PVID based on the VLAN setting.

Note: You can not enable VLAN mapping and VLAN stacking at the same time.

26.1.1 VLAN Mapping Example

In the following example figure, packets that carry VLAN ID 12 and are received on port 3 match a pre-configured VLAN mapping rule. The Switch translates the VLAN ID from 12 into 123 before forwarding the packets. Any packets carrying a VLAN tag other than 12 (such as 10) and received on port 3 will be dropped.

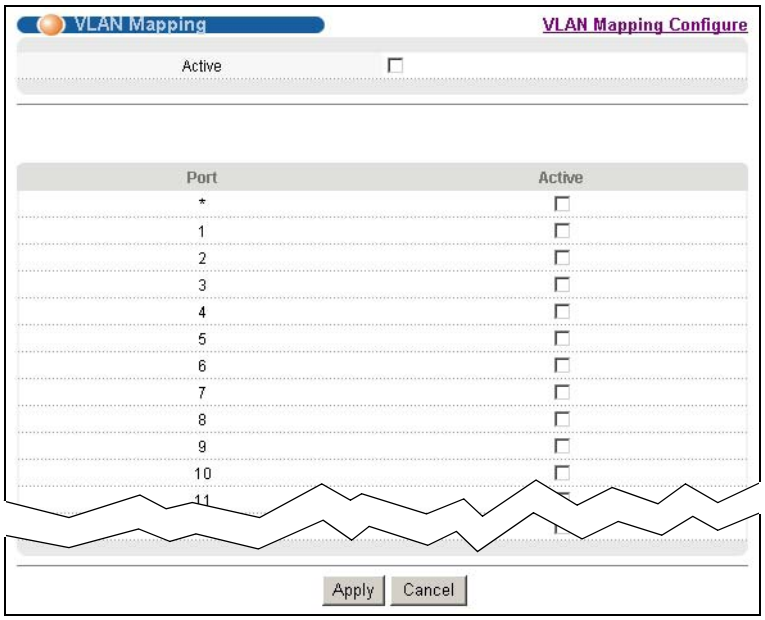
Figure 125 VLAN mapping example



26.2 Enabling VLAN Mapping

Click **Advanced Application** and then **VLAN Mapping** in the navigation panel to display the screen as shown.

Figure 126 VLAN Mapping



The following table describes the labels in this screen.

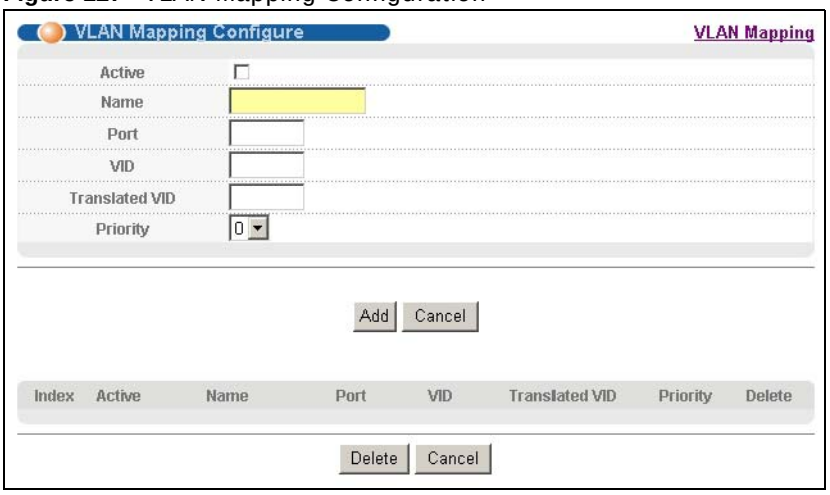
Table 96 VLAN Mapping

LABEL	DESCRIPTION
Active	Select this option to enable VLAN mapping on the Switch.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the VLAN mapping feature on this port. Clear this check box to disable the VLAN mapping feature.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

26.3 Configuring VLAN Mapping

Click the **VLAN Mapping Configure** link in the **VLAN Mapping** screen to display the screen as shown. Use this screen to enable and edit the VLAN mapping rule(s).

Figure 127 VLAN Mapping Configuration



The following table describes the labels in this screen.

Table 97 VLAN Mapping Configuration

LABEL	DESCRIPTION
Active	Check this box to activate this rule.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Port	Type a port to be included in this rule.
VID	Enter a VLAN ID from 1 to 4094. This is the VLAN tag carried in the packets and will be translated into the VID you specified in the **Translated VID** field.
Translated VID	Enter a VLAN ID (from 1 to 4094) into which the customer VID carried in the packets will be translated.
Priority	Select a priority level (from 0 to 7). This is the priority level that replaces the customer priority level in the tagged packets or adds to the untagged packets.
Add	Click **Add** to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Index	This is the number of the VLAN mapping entry in the table.
Active	This shows whether this entry is activated or not.
Name	This is the descriptive name for this rule.
Port	This is the port number to which this rule is applied.
VID	This is the customer VLAN ID in the incoming packets.
Translated VID	This is the VLAN ID that replaces the customer VLAN ID in the tagged packets.
Priority	This is the priority level that replaces the customer priority level in the tagged packets.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

27

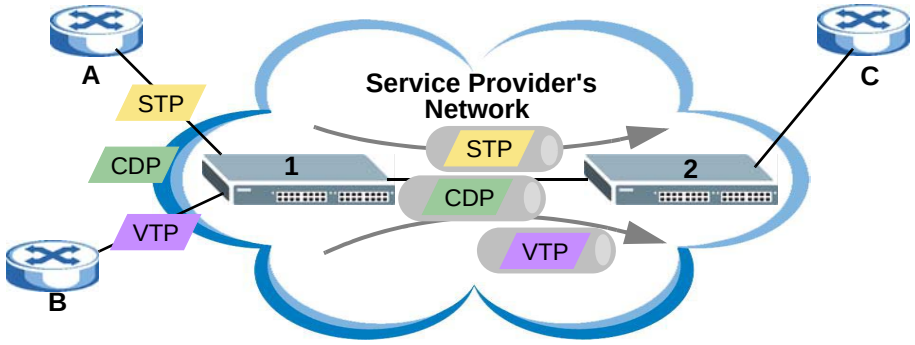
Layer 2 Protocol Tunneling

This chapter shows you how to configure layer-2 protocol tunneling on the Switch.

27.1 Layer 2 Protocol Tunneling Overview

Layer-2 protocol tunneling (L2PT) is used on the service provider's edge devices. L2PT allows edge switches (**1** and **2** in the following figure) to tunnel layer-2 STP (Spanning Tree Protocol), CDP (Cisco Discovery Protocol) and VTP (VLAN Trunking Protocol) packets between customer switches (**A**, **B** and **C** in the following figure) connected through the service provider's network. The edge switch encapsulates layer-2 protocol packets with a specific MAC address before sending them across the service provider's network to other edge switches.

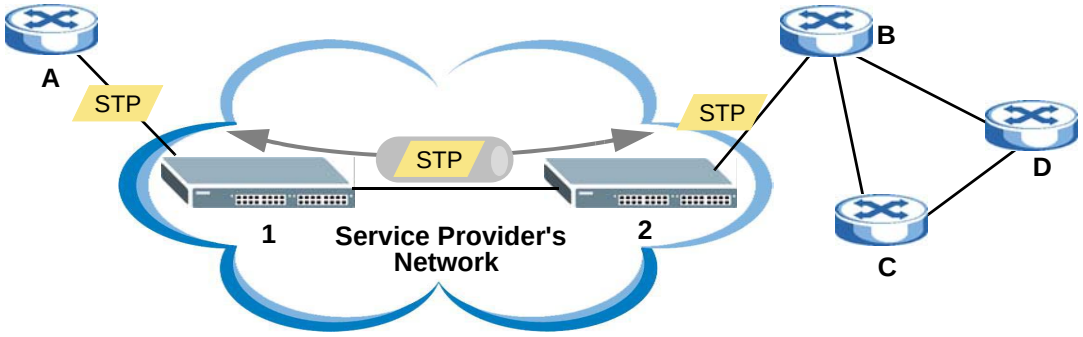
Figure 128 Layer-2 Protocol Tunneling Network Scenario



In the following example, if you enable L2PT for STP, you can have switches **A**, **B**, **C** and **D** in the same spanning tree, even though switch **A** is not directly connected to switches **B**, **C** and **D**. Topology change information can be propagated throughout the service provider's network.

To emulate a point-to-point topology between two customer switches at different sites, such as **A** and **B**, you can enable protocol tunneling on edge switches **1** and **2** for PAgP (Port Aggregation Protocol), LACP or UDLD (UniDirectional Link Detection).

Figure 129 L2PT Network Example



27.1.1 Layer-2 Protocol Tunneling Mode

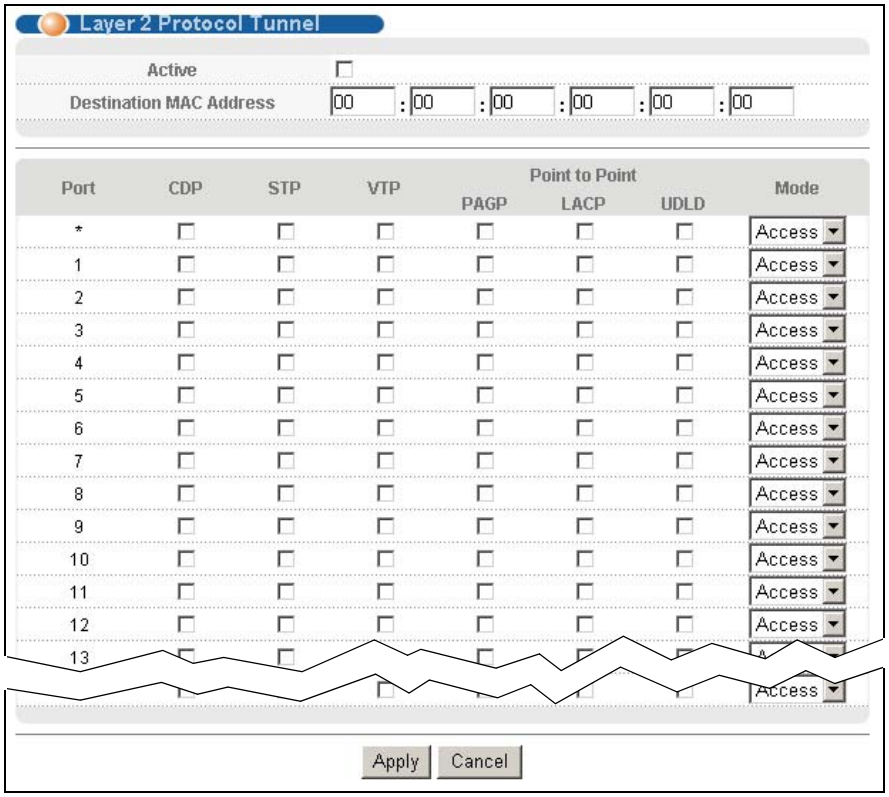
Each port can have two layer-2 protocol tunneling modes, **Access** and **Tunnel**.

- The **Access** port is an ingress port on the service provider's edge device (**1** or **2** in Figure 129 on page 229) and connected to a customer switch (**A** or **B**). Incoming layer-2 protocol packets received on an access port are encapsulated and forwarded to the tunnel ports.
- The **Tunnel** port is an egress port at the edge of the service provider's network and connected to another service provider's switch. Incoming encapsulated layer-2 protocol packets received on a tunnel port are decapsulated and sent to an access port.

27.2 Configuring Layer 2 Protocol Tunneling

Click **Advanced Application** > **Layer 2 Protocol Tunneling** in the navigation panel to display the screen as shown.

Figure 130 Advanced Application > Layer 2 Protocol Tunneling



The following table describes the labels in this screen.

Table 98 Advanced Application > Layer 2 Protocol Tunneling

LABEL	DESCRIPTION
Active	Select this to enable layer-2 protocol tunneling on the Switch.
Destination MAC Address	Specify an MAC address with which the Switch uses to encapsulate the layer-2 protocol packets by replacing the destination MAC address in the packets. Note: The MAC address can be either a unicast MAC address or multicast MAC address. If you use a unicast MAC address, make sure the MAC address does not exist in the address table of a switch on the service provider's network. Note: All the edge switches in the service provider's network should be set to use the same MAC address for encapsulation.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
CDP	Select this option to have the Switch tunnel CDP (Cisco Discovery Protocol) packets so that other Cisco devices can be discovered through the service provider's network.

Table 98 Advanced Application > Layer 2 Protocol Tunneling (continued)

LABEL	DESCRIPTION
STP	Select this option to have the Switch tunnel STP (Spanning Tree Protocol) packets so that STP can run properly across the service provider's network and spanning trees can be set up based on bridge information from all (local and remote) networks.
VTP	Select this option to have the Switch tunnel VTP (VLAN Trunking Protocol) packets so that all customer switches can use consistent VLAN configuration through the service provider's network.
Point to Point	The Switch supports PAgP (Port Aggregation Protocol), LACP (Link Aggregation Control Protocol) and UDLD (UniDirectional Link Detection) tunneling for a point-to-point topology. Both PAgP and UDLD are Cisco's proprietary data link layer protocols. PAgP is similar to LACP and used to set up a logical aggregation of Ethernet ports automatically. UDLD is to determine the link's physical status and detect a unidirectional link.
PAGP	Select this option to have the Switch send PAgP packets to a peer to automatically negotiate and build a logical port aggregation.
LACP	Select this option to have the Switch send LACP packets to a peer to dynamically creates and manages trunk groups.
UDLD	Select this option to have the Switch send UDLD packets to a peer's port it connected to monitor the physical status of a link.
Mode	Select **Access** to have the Switch encapsulate the incoming layer-2 protocol packets and forward them to the tunnel port(s). Select **Access** for ingress ports at the edge of the service provider's network. Note: You can enable L2PT services for STP, LACP, VTP, CDP, UDLD, and PAGP on the access port(s) only. Select **Tunnel** for egress ports at the edge of the service provider's network. The Switch decapsulates the encapsulated layer-2 protocol packets received on a tunnel port by changing the destination MAC address to the original one, and then forward them to an access port. If the service(s) is not enabled on an access port, the protocol packets are dropped.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

28

sFlow

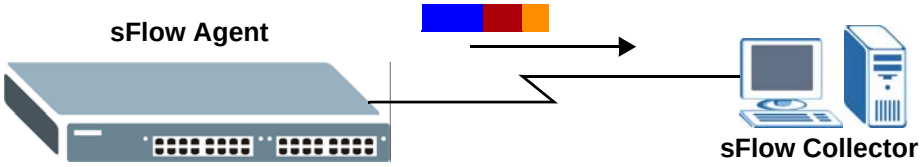
This chapter shows you how to configure sFlow to have the Switch monitor traffic in a network and send information to an sFlow collector for analysis.

28.1 sFlow Overview

sFlow (RFC 3176) is a standard technology for monitoring switched networks. An sFlow agent embedded on a switch or router gets sample data and packet statistics from traffic forwarded through its ports. The sFlow agent then creates sFlow data and sends it to an sFlow collector. The sFlow collector is a server that collects and analyzes sFlow datagram. An sFlow datagram includes packet header, input and output interface, sampling process parameters and forwarding information.

sFlow minimizes impact on CPU load of the Switch as it analyzes sample data only. sFlow can continuously monitor network traffic and create reports for network performance analysis and troubleshooting. For example, you can use it to know which IP address or which type of traffic caused network congestion.

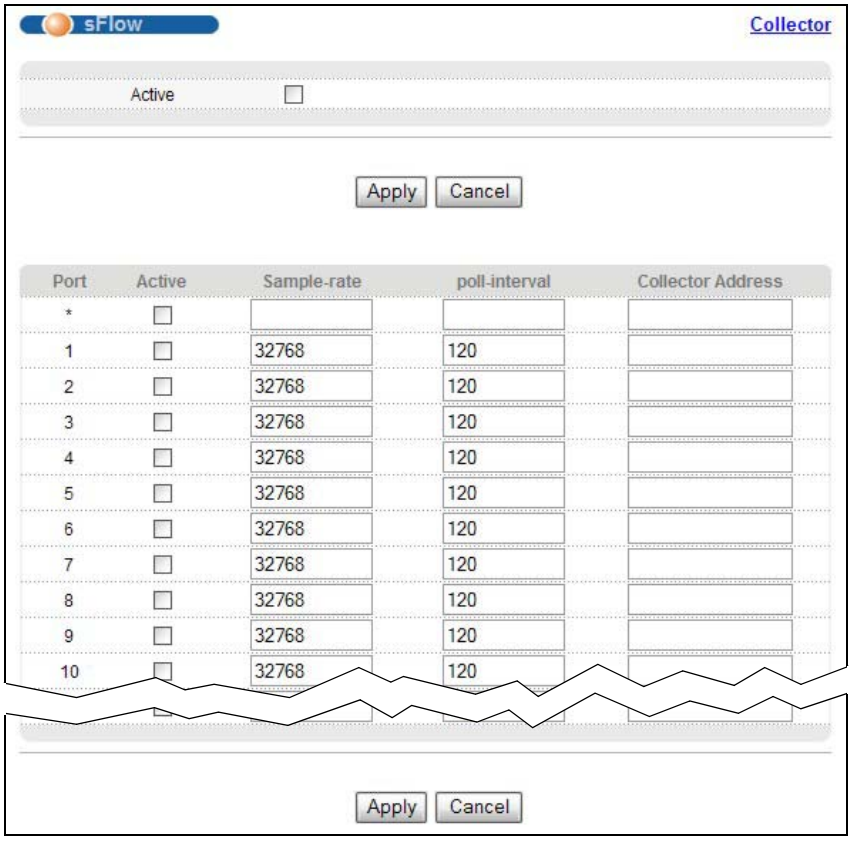
Figure 131 sFlow Application



28.2 sFlow Port Configuration

Click **Advanced Application** > **sFlow** in the navigation panel to display the screen as shown.

Figure 132 Advanced Application > sFlow



The following table describes the labels in this screen.

Table 99 Advanced Application > sFlow

LABEL	DESCRIPTION
Active	Select this to enable the sFlow agent on the Switch.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to allow the Switch to monitor traffic on this port and generate and send sFlow datagram to the specified collector.
Sample-rate	Enter a number (N) from 256 to 65535. The Switch captures every one out of N packets for this port and creates sFlow datagram.
poll-interval	Specify a time interval (from 20 to 120 in seconds) the Switch waits before sending the sFlow datagram and packet counters for this port to the collector.

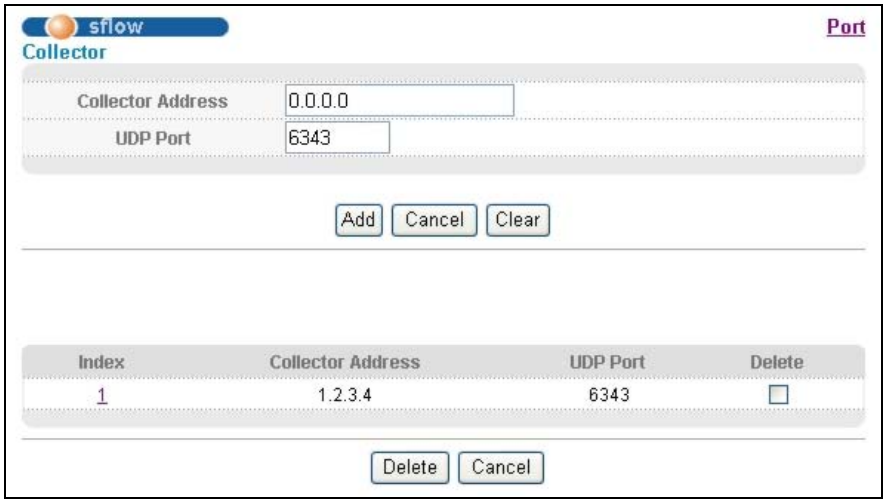
Table 99 Advanced Application > sFlow (continued)

LABEL	DESCRIPTION
Collector Address	Enter the IP address of the sFlow collector. Note: You must have the sFlow collector already configured in the **sFlow > Collector** screen. The sFlow collector does not need to be in the same subnet as the Switch, but it must be accessible from the Switch. Note: Configure UDP port 6343 (the default) on a NAT router to allow port forwarding if the collector is behind a NAT router. Configure a firewall rule for UDP port 6343 (the default) to allow incoming traffic if the collector is behind a firewall.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

28.2.1 sFlow Collector Configuration

Click the **Collector** link in the **sFlow** screen to display the screen as shown. You can configure up to four sFlow collectors in this screen. You may want to configure more than one collector if the traffic load to be monitored is more than one collector can manage.

Figure 133 Advanced Application > sFlow > Collector



The following table describes the labels in this screen.

Table 100 Advanced Application > sFlow > Collector

LABEL	DESCRIPTION
Collector Address	Enter the IP address of the sFlow collector.
UDP Port	Enter a UDP port number the Switch uses to send sFlow datagram to the collector. If you change the port here, make sure you change it on the collector, too. The default port is 6343.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.

Table 100 Advanced Application > sFlow > Collector (continued)

LABEL	DESCRIPTION
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This field displays the index number of this entry.
Collector Address	This field displays IP address of the sFlow collector.
UDP Port	This field displays port number the Switch uses to send sFlow datagram to the collector.
Delete	Check the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button.
Cancel	Click **Cancel** to begin configuring this screen afresh.

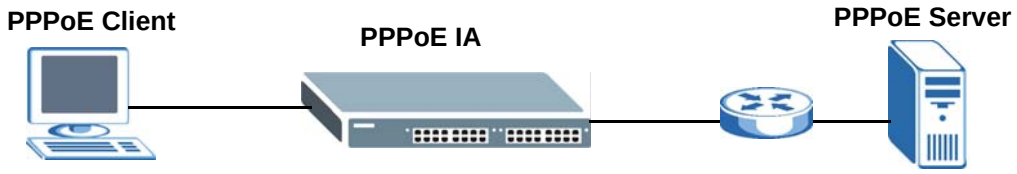
29

PPPoE

This chapter describes how the Switch gives a PPPoE termination server additional information that the server can use to identify and authenticate a PPPoE client.

29.1 PPPoE Intermediate Agent Overview

A PPPoE Intermediate Agent (PPPoE IA) is deployed between a PPPoE server and PPPoE clients. It helps the PPPoE server identify and authenticate clients by adding subscriber line specific information to PPPoE discovery packets from clients on a per-port or per-port-per-VLAN basis before forwarding them to the PPPoE server.



29.1.1 PPPoE Intermediate Agent Tag Format

If the PPPoE Intermediate Agent is enabled, the Switch adds a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients. This tag is defined in RFC 2516 and has the following format for this feature.

Table 101 PPPoE Intermediate Agent Vendor-specific Tag Format

Tag_Type (0x0105)	Tag_Len	Value	i1	i2

The Tag_Type is 0x0105 for vendor-specific tags, as defined in RFC 2516. The Tag_Len indicates the length of Value, i1 and i2. The Value is the 32-bit number 0x00000DE9, which stands for the “ADSL Forum” IANA entry. i1 and i2 are PPPoE intermediate agent sub-options, which contain additional information about the PPPoE client.

29.1.2 Sub-Option Format

There are two types of sub-option: “Agent Circuit ID Sub-option” and “Agent Remote ID Sub-option”. They have the following formats.

Table 102 PPPoE IA Circuit ID Sub-option Format: User-defined String

SubOpt	Length	Value
0x01 (1 byte)	N (1 byte)	String (63 bytes)

Table 103 PPPoE IA Remote ID Sub-option Format

SubOpt	Length	Value
0x02 (1 byte)	N (1 byte)	MAC Address or String (63 bytes)

The 1 in the first field identifies this as an Agent Circuit ID sub-option and 2 identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field. The Switch takes the Circuit ID string you manually configure for a VLAN on a port as the highest priority and the Circuit ID string for a port as the second priority. In addition, the Switch puts the PPPoE client's MAC address into the Agent Remote ID Sub-option if you do not specify any user-defined string.

29.1.2.1 Flexible Circuit ID Syntax with Identifier String and Variables

If you do not configure a Circuit ID string for a VLAN on a specific port or for a specific port, the Switch adds the user-defined identifier string and variables into the Agent Circuit ID Sub-option. The variables can be the slot ID of the PPPoE client, the port number of the PPPoE client and/or the VLAN ID on the PPPoE packet.

The identifier-string, slot ID, port number and VLAN ID are separated from each other by a pound key (#), semi-colon (;), period (.), comma (,), forward slash (/) or space. An Agent Circuit ID Sub-option example is "Switch/07/0123" and indicates the PPPoE packets come from a PPPoE client which is connected to the Switch's port 7 and belong to VLAN 123.

Table 104 PPPoE IA Circuit ID Sub-option Format: Using Identifier String and Variables

SubOpt	Length	Value						
0x01 (1 byte)	N (1 byte)	Identifier String (53 byte)	delimiter (1 byte)	Slot ID (1 byte)	delimiter (1 byte)	Port No (2 byte)	delimiter (1 byte)	VLAN ID (4 bytes)

29.1.2.2 WT-101 Default Circuit ID Syntax

If you do not configure a Circuit ID string for a specific VLAN on a port or for a specific port, and disable the flexible Circuit ID syntax in the **PPPoE > Intermediate Agent** screen, the Switch automatically generates a Circuit ID string according to the default Circuit ID syntax which is defined in the DSL Forum Working Text (WT)-101. The default access node identifier is the host name of the PPPoE intermediate agent and the eth indicates "Ethernet".

Table 105 PPPoE IA Circuit ID Sub-option Format: Defined in WT-101

SubOpt	Length	Value								
0x01 (1 byte)	N (1 byte)	Access Node Identifier (20 byte)	Space (1 byte)	eth (3 byte)	Space (1 byte)	Slot ID (1 byte)	/ (1 byte)	Port No (2 byte)	: (1 byte)	VLAN ID (4 bytes)

29.1.3 Port State

Every port is either a trusted port or an untrusted port for the PPPoE intermediate agent. This setting is independent of the trusted/untrusted setting for DHCP snooping or ARP inspection. You can also specify the agent sub-options (circuit ID and remote ID) that the Switch adds to PADI and PADR packets from PPPoE clients.

Trusted ports are connected to PPPoE servers.

- If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports.
- If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s).

Note: The Switch will drop all PPPoE discovery packets if you enable the PPPoE intermediate agent and there are no trusted ports.

Untrusted ports are connected to subscribers.

- If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s).
- The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.

29.2 The PPPoE Screen

Use this screen to configure the PPPoE Intermediate Agent on the Switch.

Click **Advanced Application** > **PPPoE** in the navigation panel to display the screen as shown. Click **Click Here** to go to the **Intermediate Agent** screen.

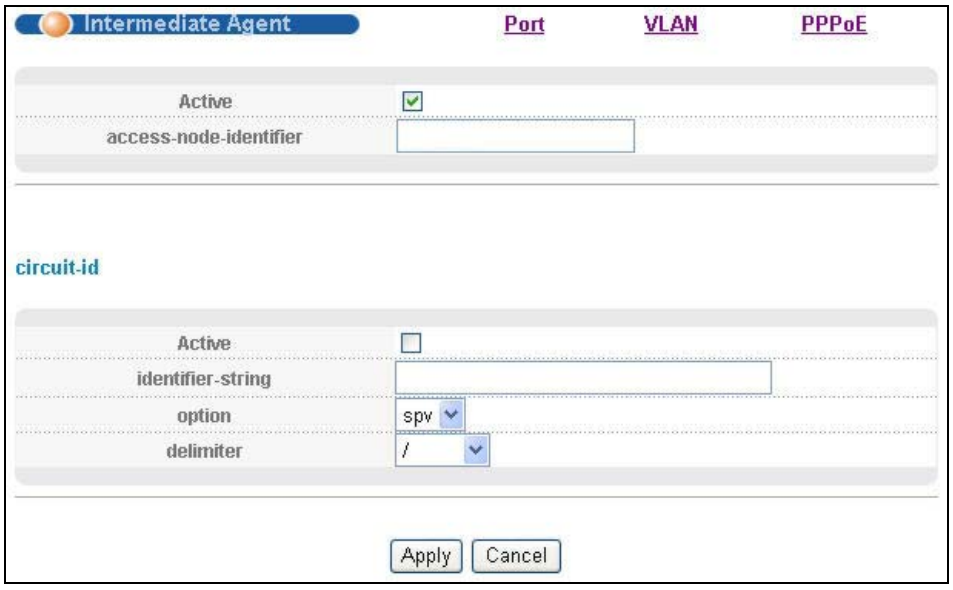
Figure 134 Advanced Application > PPPoE Intermediate Agent

29.3 PPPoE Intermediate Agent

Use this screen to configure the Switch to give a PPPoE termination server additional subscriber information that the server can use to identify and authenticate a PPPoE client.

Click **Advanced Application** > **PPPoE > Intermediate Agent** in the navigation panel to display the screen as shown.

Figure 135 Advanced Application > PPPoE > Intermediate Agent



The following table describes the labels in this screen.

Table 106 Advanced Application > PPPoE > Intermediate Agent

LABEL	DESCRIPTION
Active	Select this option to enable the PPPoE intermediate agent globally on the Switch.
access-node-identifier	Enter up to 20 ASCII characters to identify the PPPoE intermediate agent. Hyphens (-) and spaces are also allowed. The default is the Switch's host name.
circuit-id	Use this section to configure the Circuit ID field in the PADI and PADR packets. The Circuit ID you configure for a specific port or for a specific VLAN on a port has priority over this. The Circuit ID you configure for a specific port (in the **Advanced Application > PPPoE > Intermediate Agent > Port** screen) or for a specific VLAN on a port (in the **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN** screen) has priority over this. That means, if you also want to configure PPPoE IA Per-Port or Per-Port Per-VLAN setting, leave the fields here empty and configure circuit-id and remote-id in the Per-Port or Per-Port Per-VLAN screen.
Active	Select this option to have the Switch add the user-defined identifier string and variables (specified in the **option** field) to PADI or PADR packets from PPPoE clients. If you leave this option unselected and do not configure any Circuit ID string (using CLI commands) on the Switch, the Switch will use the string specified in the **access-node-identifier** field.
identifier-string	Specify a string that the Switch adds in the Agent Circuit ID sub-option. You can enter up to 53 ASCII characters. Spaces are allowed.
option	Select the variables that you want the Switch to generate and add in the Agent Circuit ID sub-option. The variable options include **sp**, **sv**, **pv** and **spv** which indicate combinations of slot-port, slot-VLAN, port-VLAN and slot-port-VLAN respectively. The Switch enters a zero into the PADI and PADR packets for the slot value.
delimiter	Select a delimiter to separate the identifier-string, slot ID, port number and/or VLAN ID from each other. You can use a pound key (**#**), semi-colon (**;**), period (**.**), comma (**,**), forward slash (**/**) or space.

Table 106 Advanced Application > PPPoE > Intermediate Agent (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

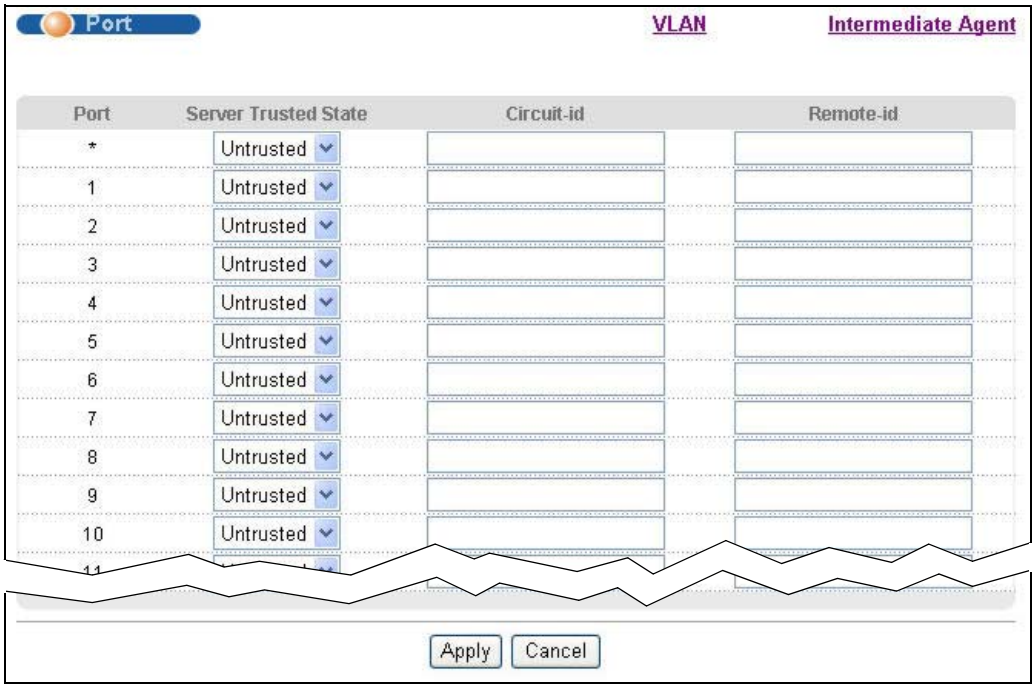
29.3.1 PPPoE IA Per-Port

Use this screen to specify whether individual ports are trusted or untrusted ports and have the Switch add extra information to PPPoE discovery packets from PPPoE clients on a per-port basis.

Note: The Switch will drop all PPPoE packets if you enable the PPPoE Intermediate Agent on the Switch and there are no trusted ports.

Click the **Port** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 136 Advanced Application > PPPoE > Intermediate Agent > Port



The following table describes the labels in this screen.

Table 107 Advanced Application > PPPoE > Intermediate Agent > Port

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 107 Advanced Application > PPPoE > Intermediate Agent > Port (continued)

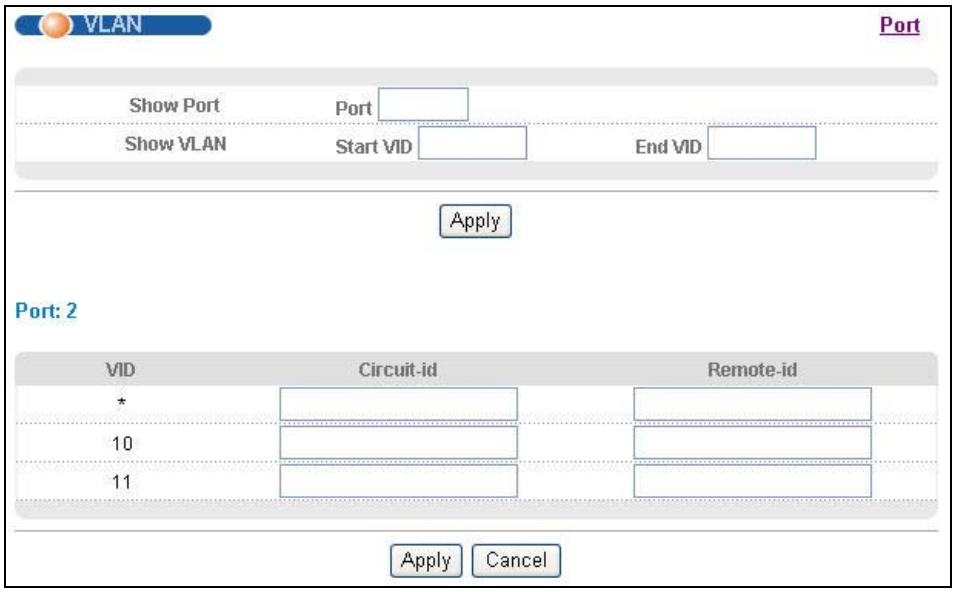
LABEL	DESCRIPTION
Server Trusted State	Select whether this port is a trusted port (**Trusted**) or an untrusted port (**Untrusted**). Trusted ports are uplink ports connected to PPPoE servers. • If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports. • If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s). Untrusted ports are downlink ports connected to subscribers. • If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s). • The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.
Circuit-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. The Circuit ID you configure for a specific VLAN on a port (in the **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN** screen) has the highest priority.
Remote-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Remote ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. If you do not specify a string here or in the **Remote-id** field for a VLAN on a port, the Switch automatically uses the PPPoE client's MAC address. The Remote ID you configure for a specific VLAN on a port (in the **Advanced Application > PPPoE > Intermediate Agent > Port > VLAN** screen) has the highest priority.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

29.3.2 PPPoE IA Per-Port Per-VLAN

Use this screen to configure PPPoE IA settings that apply to a specific VLAN on a port.

Click the **VLAN** link in the **Intermediate Agent > Port** screen to display the screen as shown.

Figure 137 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN



The following table describes the labels in this screen.

Table 108 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN

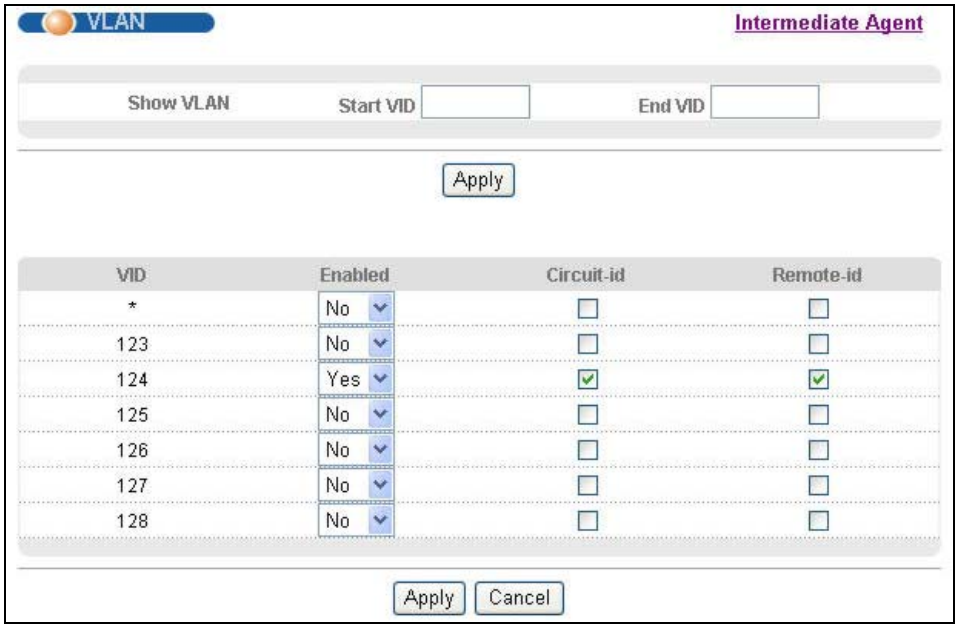
LABEL	DESCRIPTION
Show Port	Enter a port number to show the PPPoE Intermediate Agent settings for the specified VLAN(s) on the port.
Show VLAN	Use this section to specify the VLANs you want to configure in the section below.
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Apply	Click **Apply** to display the specified range of VLANs in the section below.
Port	This field displays the port number specified above.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Note: Changes in this row are copied to all the VLANs as soon as you make them.
Circuit-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for this VLAN on the specified port. Spaces are allowed. The Circuit ID you configure here has the highest priority.
Remote-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Remote ID sub-option for this VLAN on the specified port. Spaces are allowed. If you do not specify a string here or in the **Remote-id** field for a specific port, the Switch automatically uses the PPPoE client's MAC address. The Remote ID you configure here has the highest priority.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

29.3.3 PPPoE IA for VLAN

Use this screen to set whether the PPPoE Intermediate Agent is enabled on a VLAN and whether the Switch appends the Circuit ID and/or Remote ID to PPPoE discovery packets from a specific VLAN.

Click the **VLAN** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 138 Advanced Application > PPPoE > Intermediate Agent > VLAN



The following table describes the labels in this screen.

Table 109 Advanced Application > PPPoE > Intermediate Agent > VLAN

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to configure in the section below.
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Apply	Click **Apply** to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the ***** VLAN, the settings are applied to all VLANs.
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Note: Changes in this row are copied to all the VLANs as soon as you make them.
Enabled	Select this option to turn on the PPPoE Intermediate Agent on a VLAN.
Circuit-id	Select this option to make the Circuit ID settings for a specific VLAN take effect.
Remote-id	Select this option to make the Remote ID settings for a specific VLAN take effect.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

30

Error Disable

This chapter shows you how to configure the rate limit for control packets on a port, and set the Switch to take an action (such as to shut down a port or stop sending packets) on a port when the Switch detects a pre-configured error. It also shows you how to configure the Switch to automatically undo the action after the error is gone.

30.1 CPU Protection Overview

Switches exchange protocol control packets in a network to get the latest networking information. If a switch receives large numbers of control packets, such as ARP, BPDU or IGMP packets, which are to be processed by the CPU, the CPU may become overloaded and be unable to handle regular tasks properly.

The CPU protection feature allows you to limit the rate of ARP, BPDU and IGMP packets to be delivered to the CPU on a port. This enhances the CPU efficiency and protects against potential DoS attacks or errors from other network(s). You then can choose to drop control packets that exceed the specified rate limit or disable a port on which the packets are received.

30.2 Error-Disable Recovery Overview

Some features, such as loop guard or CPU protection, allow the Switch to shut down a port or discard specific packets on a port when an error is detected on the port. For example, if the Switch detects that packets sent out the port(s) loop back to the Switch, the Switch can shut down the port(s) automatically. After that, you need to enable the port(s) or allow the packets on a port manually via the web configurator or the commands. With error-disable recovery, you can set the disabled port(s) to become active or start receiving the packets again after the time interval you specify.

30.3 The Error Disable Screen

Use this screen to configure error disable related settings. Click **Advanced Application > Errdisable** in the navigation panel to open the following screen.

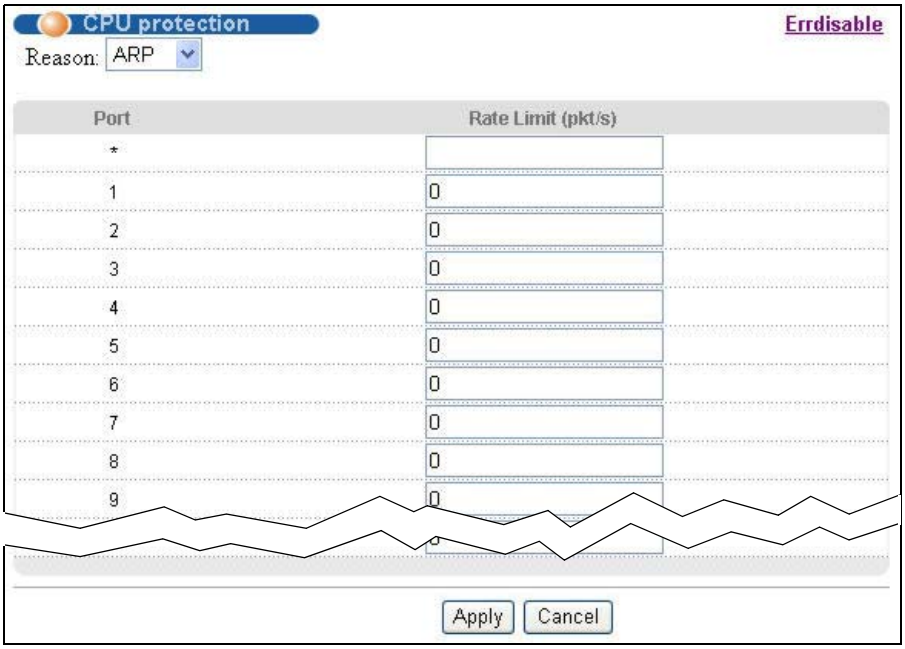
Figure 139 Advanced Application > Errdisable

30.4 CPU Protection Configuration

Use this screen to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the Switch can receive or transmit on a port. Click the **Click Here** link next to **CPU protection** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Note: After you configure this screen, make sure you also enable error detection for the specific control packets in the **Advanced Application** > **Errdisable** > **Errdisable Detect** screen.

Figure 140 Advanced Application > Errdisable > CPU protection



The following table describes the labels in this screen.

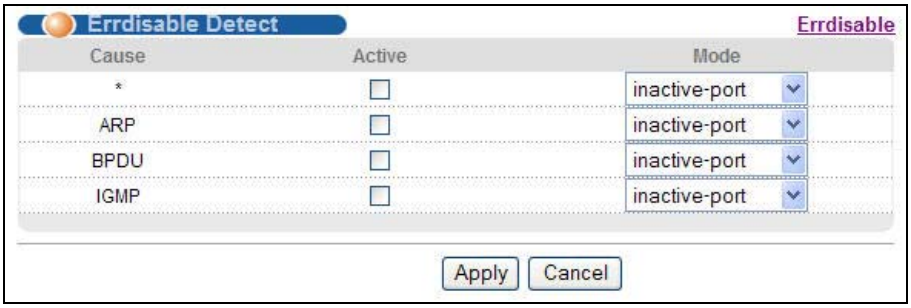
Table 110 Advanced Application > Errdisable > CPU protection

LABEL	DESCRIPTION
Reason	Select the type of control packet you want to configure here.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Note: Changes in this row are copied to all the ports as soon as you make them.
Rate Limit (pkt/s)	Enter a number from 0 to 256 to specify how many control packets this port can receive or transmit per second. **0** means no rate limit. You can configure the action that the Switch takes when the limit is exceeded. See Section 30.5 on page 246 for detailed information.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

30.5 Error-Disable Detect Configuration

Use this screen to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded. Click the **Click Here** link next to **Errdisable Detect** link in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 141 Advanced Application > Errdisable > Errdisable Detect



The following table describes the labels in this screen.

Table 111 Advanced Application > Errdisable > Errdisable Detect

LABEL	DESCRIPTION
Cause	This field displays the types of control packet that may cause CPU overload.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Note: Changes in this row are copied to all the entries as soon as you make them.
Active	Select this option to have the Switch detect if the configured rate limit for a specific control packet is exceeded and take the action selected below.

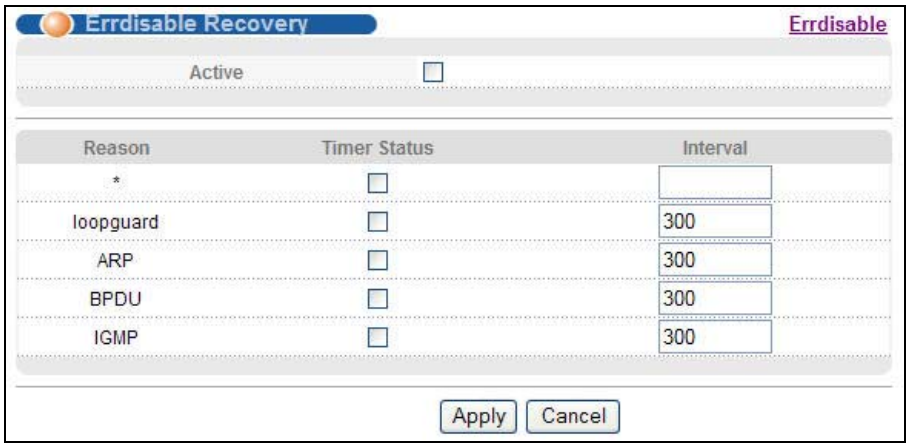
Table 111 Advanced Application > Errdisable > Errdisable Detect (continued)

LABEL	DESCRIPTION
Mode	Select the action that the Switch takes when the number of control packets exceed the rate limit on a port, set in the **Advanced Application > Errdisable > CPU protection** screen. • **inactive-port** - The Switch disables the port on which the control packets are received. • **inactive-reason** - The Switch bypasses the processing of the specified control packets (such as ARP or IGMP packets), or drops all the specified control packets (such as BPDU) on the port. • **rate-limitation** - The Switch drops the additional control packets the port has to handle in every one second.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

30.6 Error-Disable Recovery Configuration

Use this screen to to configure the Switch to automatically undo an action after the error is gone. Click the **Click Here** link next to **Errdisable Recovery** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 142 Advanced Application > Errdisable > Errdisable Recovery



The following table describes the labels in this screen.

Table 112 Advanced Application > Errdisable > Errdisable Recovery

LABEL	DESCRIPTION
Active	Select this option to turn on the error-disable recovery function on the Switch.
Reason	This field displays the supported features that allow the Switch to shut down a port or discard packets on a port according to the feature requirements and what action you configure.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Note: Changes in this row are copied to all the entries as soon as you make them.

Table 112 Advanced Application > Errdisable > Errdisable Recovery (continued)

LABEL	DESCRIPTION
Timer Status	Select this option to allow the Switch to wait for the specified time interval to activate a port or allow specific packets on a port, after the error was gone. Deselect this option to turn off this rule.
Interval	Enter the number of seconds (from 30 to 2592000) for the time interval.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

31

Private VLAN

31.1 Private VLAN Overview

Use private VLAN if you want you to block traffic between ports in the same VLAN. **Community** and **Isolated** VLANs are secondary private VLANs that must be associated with a **Primary** private VLAN.

- **Primary**: Ports in a **Primary** VLAN are promiscuous and they can communicate with all promiscuous ports in the same primary VLAN, and all ports in associated community and isolated VLANs. They cannot communicate with ports in different primary VLANs.
- **Community**: Ports in a **Community** VLAN can communicate with promiscuous ports in an associated **Primary** VLAN and other community ports in the same **Community** VLAN. They cannot communicate with ports in **Isolated** VLANs, non-associated **Primary** VLAN promiscuous ports nor community ports in different **Community** VLANs.
- **Isolated**: Ports in an **Isolated** VLAN can communicate with promiscuous ports in an associated **Primary** VLAN only. They cannot communicate with other isolated ports in the same **Isolated** VLAN, non-associated **Primary** VLAN promiscuous ports nor any community ports.

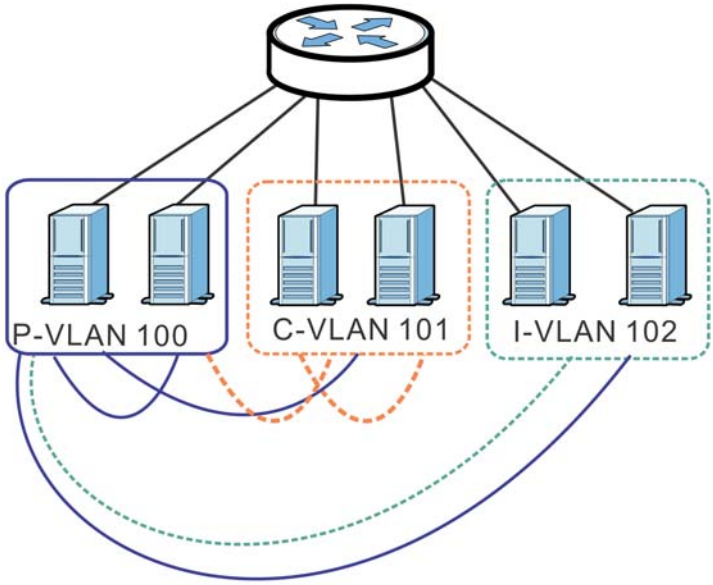


Table 113 PVLAN Graphic Key

LABEL	DESCRIPTION
P-VLAN 100	Primary private VLAN

Table 113 PVLAN Graphic Key (continued)

LABEL	DESCRIPTION
C-VLAN 101	Community private VLAN
I-VLAN 102	Isolated private VLAN

Tagged Private VLANs can span switches but trunking ports must be VLAN-trunking ports - see **Advanced > VLAN Status > VLAN Port Setting**.

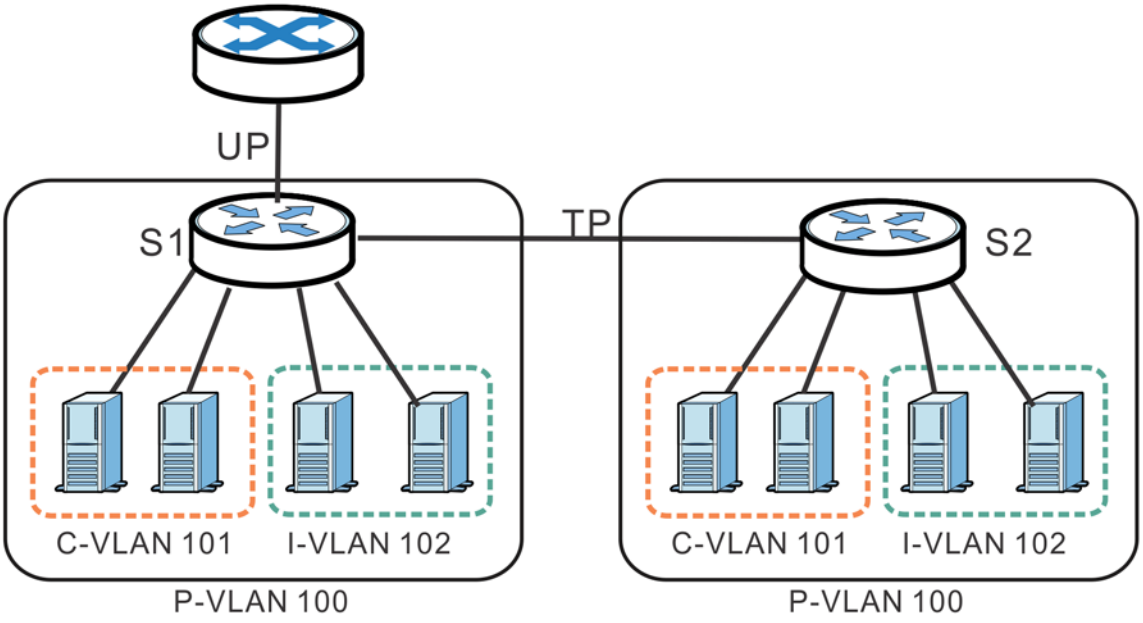


Table 114 Spanning PVLAN Graphic Key

LABEL	DESCRIPTION
UP	Uplink promiscuous port
TP	VLAN-trunking ports
S1, S2	Switch 1, Switch 2
P-VLAN 100	Primary private VLAN with VLAN ID tag of 100
C-VLAN 101	Community private VLAN with VLAN ID tag of 101
I-VLAN 102	Isolated private VLAN with VLAN ID tag of 102

This is the communication process if primary VLAN **P-VLAN 100** is associated with community VLAN **C-VLAN 101** and isolated VLAN **I-VLAN 102**.

- Promiscuous ports in **P-VLAN 100** can communicate with all ports in **P-VLAN 100** including community ports in **C-VLAN 101** and isolated ports in **I-VLAN 102**.
- Community ports in **C-VLAN 101** can communicate with promiscuous ports in **P-VLAN 100** and other commuity ports in **C-VLAN 101**. They cannot communicate with isolated ports in **I-VLAN 102**.
- Isolated ports can communicate with promiscuous ports in **P-VLAN 100**. They cannot communicate with other isolated ports in **I-VLAN 102** nor community ports in **C-VLAN 101**.

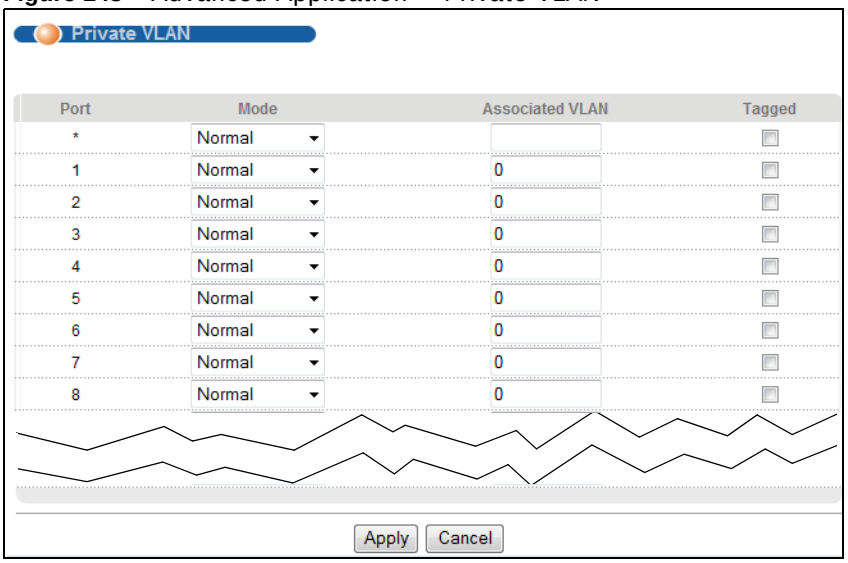
Note: **Isolation** in **VLAN > VLAN Port Setting** (see Section 7.5.4 on page 88) has a higher priority than private VLAN settings, so promiscuous ports with **Isolation** in **VLAN > VLAN Port Setting** enabled will not be able to communicate with each other.

31.1.1 Configuration

You must go to the **Static VLAN** screen first (see Section on page 98) to create VLAN IDs for **Primary**, **Isolated** or **Community** VLANs.

Click **Advanced Application > Private VLAN** to display the following screen.

Figure 143 Advanced Application > Private VLAN



The following table describes the labels in this screen.

Table 115 Advanced Application > Private VLAN

LABEL	DESCRIPTION
Port	Use the * row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Note: Changes in this row are copied to all the entries as soon as you make them.
Mode	This is the type of VLAN mapped to this port. • **Normal**: These are ports in a static VLAN. This is not a private VLAN. • **Promiscuous**: Ports in a **Primary** VLAN are **Promiscuous.** They can communicate with all ports in the **Primary** VLAN and associated **Community** and **Isolated** VLANs. They cannot communicate with **Promiscuous** ports in different primary VLANs. • **Community**: Ports in a **Community** VLAN can communicate with **Promiscuous** ports in an associated Primary VLAN and other community ports in the same **Community** VLAN. They cannot communicate with ports in an **Isolated** VLAN, non-associated **Primary** VLAN **Promiscuous** ports nor **Community** ports in different **Community** VLANs. • **Isolated:** Ports in an **Isolated** VLAN can communicate with **Promiscuous** ports in an associated **Primary** VLAN only. They cannot communicate with other **Isolated** ports in the same **Isolated** VLAN, non-associated **Primary** VLAN **Promiscuous** ports nor any **Community** ports.

Table 115 Advanced Application > Private VLAN (continued)

LABEL	DESCRIPTION
Associated VLAN	Enter the VLAN ID of a previously created VLAN here. Note: The VLAN ID and **Mode** selected here must be the same as the VLAN ID and **VLAN Type** created in **Advanced Application > VLAN > Static VLAN**.
Tagged	A VLAN ID tag identifies VLAN membership of a frame across switches. Select this if the VLAN includes ports on multiple switches. The Switch forwards tagged frames through this port; it adds the PVID to untagged frames before sending them out. Clear this if the VLAN includes ports on this Switch only. The Switch forwards untagged frames through this port; it removes the VLAN ID from tagged frames before sending them out.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

32

Static Route

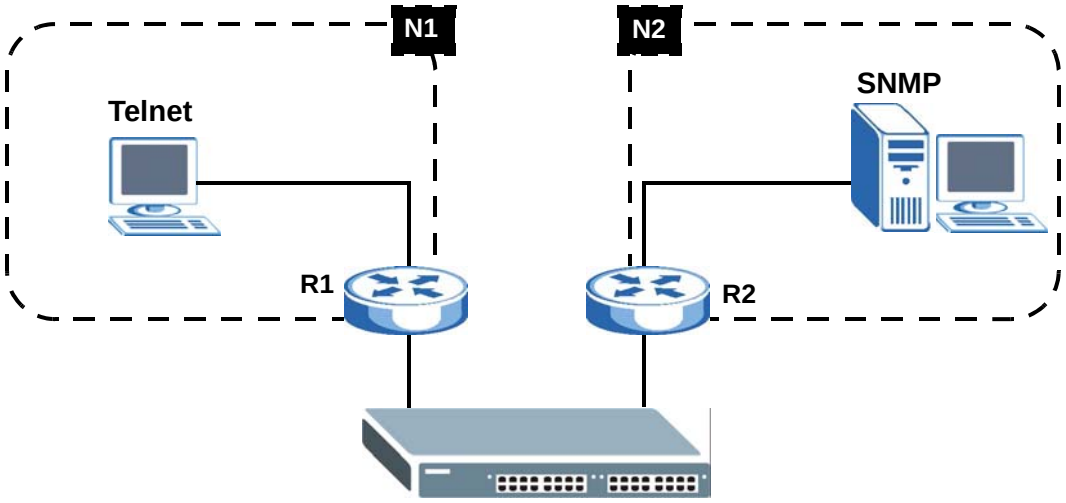
This chapter shows you how to configure static routes.

32.1 Static Routing Overview

The Switch uses IP for communication with management computers, for example using HTTP, Telnet, SSH, or SNMP. Use IP static routes to have the Switch respond to remote management stations that are not reachable through the default gateway. The Switch can also use static routes to send data to a server or device that is not reachable through the default gateway, for example when sending SNMP traps or using ping to test IP connectivity.

This figure shows a **Telnet** session coming in from network **N1**. The Switch sends reply traffic to default gateway **R1** which routes it back to the manager's computer. The Switch needs a static route to tell it to use router **R2** to send traffic to an SNMP trap server on network **N2**.

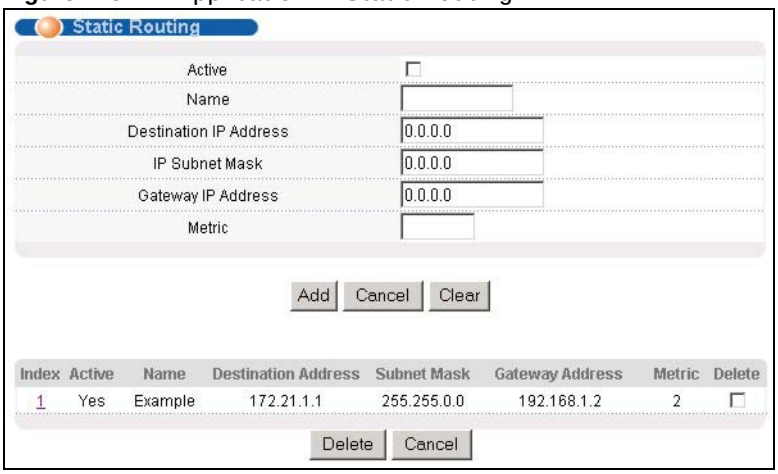
Figure 144 Static Routing Overview



32.2 Configuring Static Routing

Click **IP Application** > **Static Routing** in the navigation panel to display the screen as shown.

Figure 145 IP Application > Static Routing



The following table describes the related labels you use to create a static route.

Table 116 IP Application > Static Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 10 printable ASCII characters) for identification purposes.
Destination IP Address	This parameter specifies the IP network address of the final destination.
IP Subnet Mask	Enter the subnet mask for this destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click **Add** to insert a new static route to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the above fields to your previous configuration.
Clear	Click **Clear** to set the above fields back to the factory defaults.
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays **Yes** when the static route is activated and **No** when it is deactivated.

Table 116 IP Application > Static Routing (continued)

LABEL	DESCRIPTION
Name	This field displays the descriptive name for this route. This is for identification purposes only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

33

Differentiated Services

This chapter shows you how to configure Differentiated Services (DiffServ) on the Switch.

33.1 DiffServ Overview

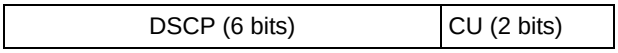
Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

33.1.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (ToS) field in the IP header. The DS field contains a 6-bit DSCP field which can define up to 64 service levels and the remaining 2 bits are defined as currently unused (CU). The following figure illustrates the DS field.

Figure 146 DiffServ: Differentiated Service Field



DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

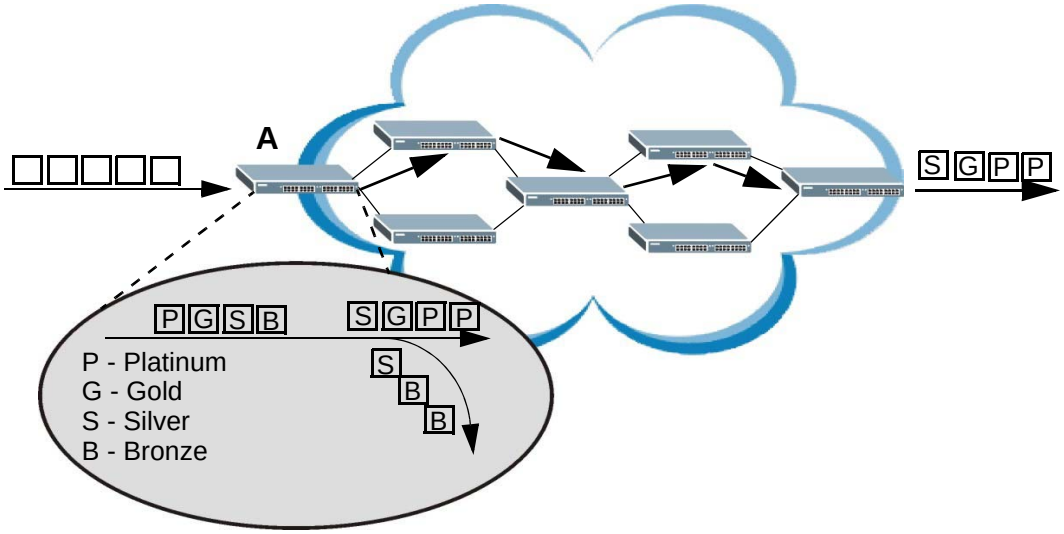
The DSCP value determines the PHB (Per-Hop Behavior), that each packet gets as it is forwarded across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

33.1.2 DiffServ Network Example

The following figure depicts a DiffServ network consisting of a group of directly connected DiffServ-compliant network devices. The boundary node (**A** in Figure 147) in a DiffServ network classifies (marks with a DSCP value) the incoming packets into different traffic flows (**Platinum**, **Gold**, **Silver**, **Bronze**) based on the configured marking rules. A network administrator can then apply

various traffic policies to the traffic flows. For example, one traffic policy would be to give higher drop precedence to one traffic flow over others. In our example packets in the **Bronze** traffic flow are more likely to be dropped when congestion occurs than the packets in the **Platinum** traffic flow as they move across the DiffServ network.

Figure 147 DiffServ Network



33.2 Two Rate Three Color Marker Traffic Policing

Traffic policing is the limiting of the input or output transmission rate of a class of traffic on the basis of user-defined criteria. Traffic policing methods measure traffic flows against user-defined criteria and identify it as either conforming, exceeding or violating the criteria.

Two Rate Three Color Marker (TRTCM, defined in RFC 2698) is a type of traffic policing that identifies packets by comparing them to two user-defined rates: the Committed Information Rate (CIR) and the Peak Information Rate (PIR). The CIR specifies the average rate at which packets are admitted to the network. The PIR is greater than or equal to the CIR. CIR and PIR values are based on the guaranteed and maximum bandwidth respectively as negotiated between a service provider and client.

Two Rate Three Color Marker evaluates incoming packets and marks them with one of three colors which refer to packet loss priority levels. High packet loss priority level is referred to as red, medium is referred to as yellow and low is referred to as green. After TRTCM is configured and DiffServ is enabled the following actions are performed on the colored packets:

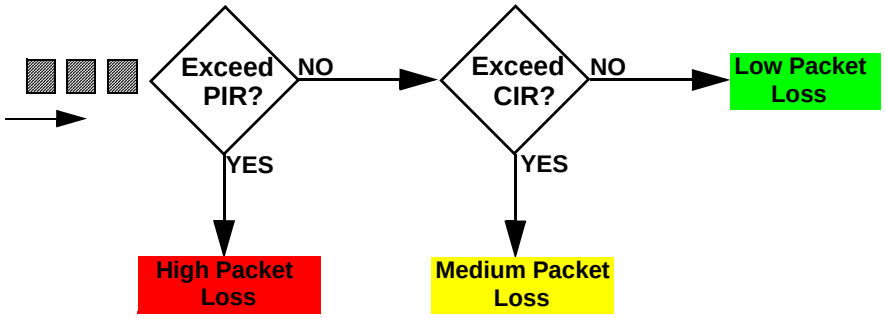
- Red (high loss priority level) packets are dropped.
- Yellow (medium loss priority level) packets are dropped if there is congestion on the network.
- Green (low loss priority level) packets are forwarded.

TRTCM operates in one of two modes: color-blind or color-aware. In color-blind mode, packets are marked based on evaluating against the PIR and CIR regardless of if they have previously been marked or not. In the color-aware mode, packets are marked based on both existing color and evaluation against the PIR and CIR. If the packets do not match any of colors, then the packets proceed unchanged.

33.2.1 TRTCM - Color-blind Mode

All packets are evaluated against the PIR. If a packet exceeds the PIR it is marked red. Otherwise it is evaluated against the CIR. If it exceeds the CIR then it is marked yellow. Finally, if it is below the CIR then it is marked green.

Figure 148 TRTCM - Color-blind Mode

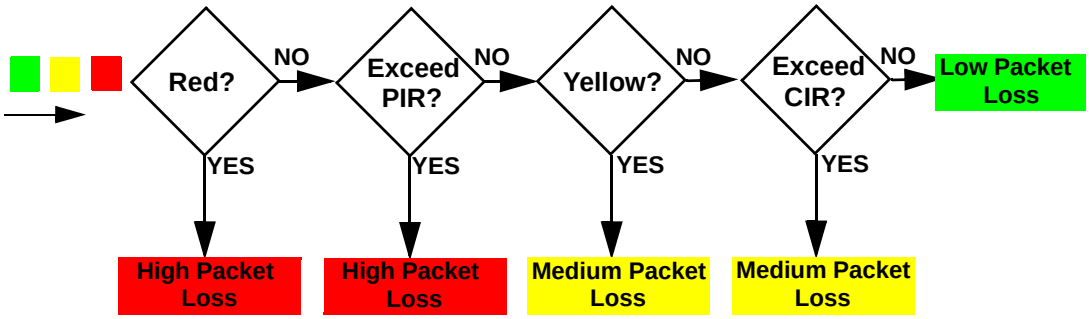


33.2.2 TRTCM - Color-aware Mode

In color-aware mode the evaluation of the packets uses the existing packet loss priority. TRTCM can increase a packet loss priority of a packet but it cannot decrease it. Packets that have been previously marked red or yellow can only be marked with an equal or higher packet loss priority.

Packets marked red (high packet loss priority) continue to be red without evaluation against the PIR or CIR. Packets marked yellow can only be marked red or remain yellow so they are only evaluated against the PIR. Only the packets marked green are first evaluated against the PIR and then if they don't exceed the PIR level are they evaluated against the CIR.

Figure 149 TRTCM - Color-aware Mode



33.3 Activating DiffServ

Activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the selected port(s).

Click **IP Application** > **DiffServ** in the navigation panel to display the screen as shown.

Figure 150 IP Application > DiffServ

The following table describes the labels in this screen.

Table 117 IP Application > DiffServ

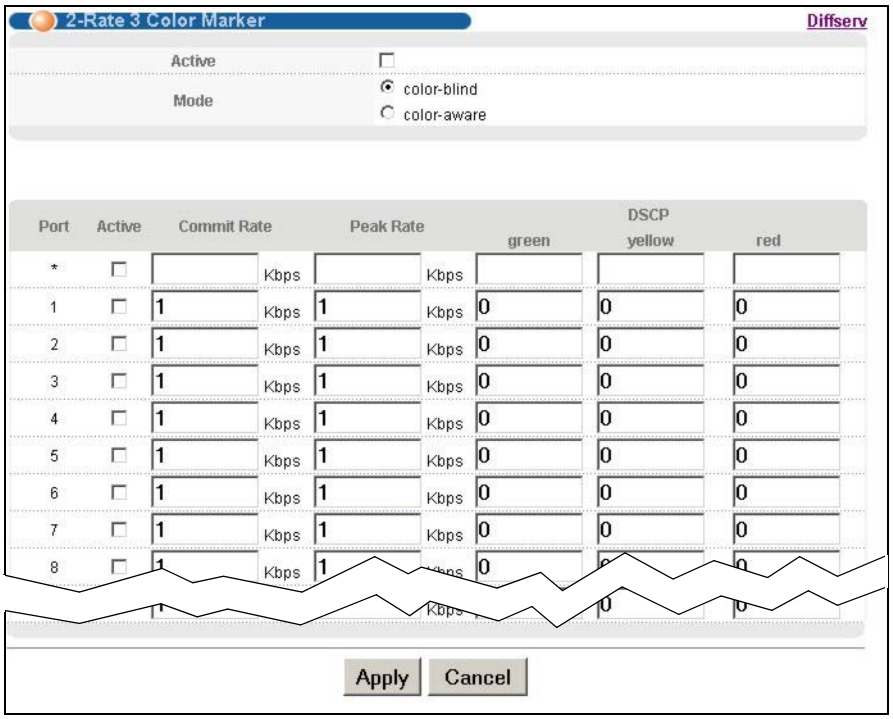
LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the Switch.
Port	This field displays the index number of a port on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select **Active** to enable DiffServ on the port.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

33.3.1 Configuring 2-Rate 3 Color Marker Settings

Use this screen to configure TRTCM settings. Click the **2-rate 3 Color Marker** link in the **DiffServ** screen to display the screen as shown next.

Note: You cannot enable both TRTCM and Bandwidth Control at the same time.

Figure 151 IP Application > DiffServ > 2-rate 3 Color Marker



The following table describes the labels in this screen.

Table 118 IP Application > DiffServ > 2-rate 3 Color Marker

LABEL	DESCRIPTION
Active	Select this to activate TRTCM (Two Rate Three Color Marker) on the Switch. The Switch evaluates and marks the packets based on the TRTCM settings. Note: You must also activate **DiffServ** on the Switch and the individual ports for the Switch to drop red (high loss priority) colored packets.
Mode	Select **color-blind** to have the Switch treat all incoming packets as uncolored. All incoming packets are evaluated against the CIR and PIR. Select **color-aware** to treat the packets as marked by some preceding entity. Incoming packets are evaluated based on their existing color. Incoming packets that are not marked proceed through the Switch.
Port	This field displays the index number of a port on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to activate TRTCM on the port.
Commit Rate	Specify the Commit Information Rate (CIR) for this port.
Peak Rate	Specify the Peak Information Rate (PIR) for this port.

Table 118 IP Application > DiffServ > 2-rate 3 Color Marker (continued)

LABEL	DESCRIPTION
DSCP	Use this section to specify the DSCP values that you want to assign to packets based on the color they are marked via TRTCM.
green	Specify the DSCP value to use for packets with low packet loss priority.
yellow	Specify the DSCP value to use for packets with medium packet loss priority.
red	Specify the DSCP value to use for packets with high packet loss priority.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

33.4 DSCP-to-IEEE 802.1p Priority Settings

You can configure the DSCP to IEEE 802.1p mapping to allow the Switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE 802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1p mapping.

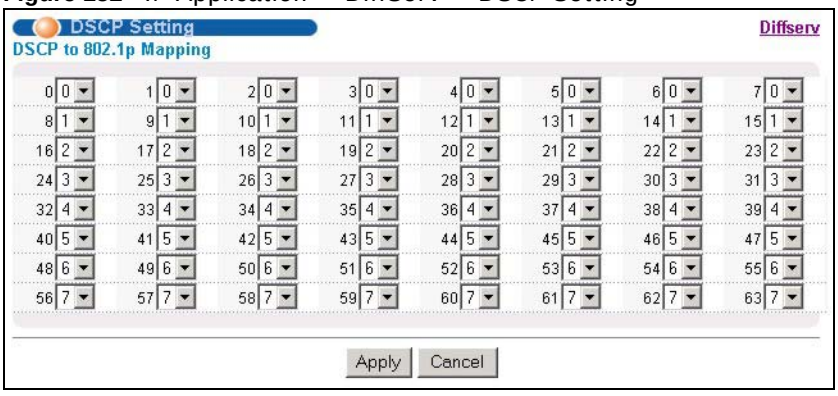
Table 119 Default DSCP-IEEE 802.1p Mapping

DSCP VALUE	0 – 7	8 – 15	16 – 23	24 – 31	32 – 39	40 – 47	48 – 55	56 – 63
IEEE 802.1p	0	1	2	3	4	5	6	7

33.4.1 Configuring DSCP Settings

To change the DSCP-IEEE 802.1p mapping, click the **DSCP Setting** link in the **DiffServ** screen to display the screen as shown next.

Figure 152 IP Application > DiffServ > DSCP Setting



The following table describes the labels in this screen.

Table 120 IP Application > DiffServ > DSCP Setting

LABEL	DESCRIPTION
0 ... 63	This is the DSCP classification identification number. To set the IEEE 802.1p priority mapping, select the priority level from the drop-down list box.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

34

DHCP

This chapter shows you how to configure the DHCP feature.

34.1 DHCP Overview

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. When you configure the Switch as a relay agent, then the Switch forwards DHCP requests to DHCP server on your network. If you don't configure the Switch as a relay agent then you must have a DHCP server in the broadcast domain of the client computers or else the client computers must be configured manually.

34.1.1 DHCP Configuration Options

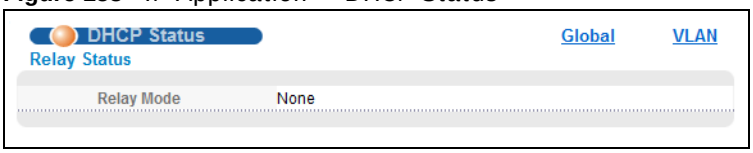
The DHCP configuration on the Switch is divided into **Global** and **VLAN** screens. The screen you should use for configuration depends on the DHCP services you want to offer the DHCP clients on your network. Choose the configuration screen based on the following criteria:

- **Global** - The Switch forwards all DHCP requests to the same DHCP server.
- **VLAN** - The Switch is configured on a VLAN by VLAN basis.

34.2 DHCP Status

Click **IP Application** > **DHCP** in the navigation panel. The **DHCP Status** screen displays.

Figure 153 IP Application > DHCP Status



The following table describes the labels in this screen.

Table 121 IP Application > DHCP Status

LABEL	DESCRIPTION
Relay Status	This section displays configuration settings related to the Switch's DHCP relay mode.
Relay Mode	This field displays: • **None** - if the Switch is not configured as a DHCP relay agent. • **Global** - if the Switch is configured as a DHCP relay agent only. • **VLAN** - followed by a VLAN ID or multiple VLAN IDs if it is configured as a relay agent for specific VLAN(s).

34.3 DHCP Relay

Configure DHCP relay on the Switch if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the Switch helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the Switch.

The Switch can be configured as a global DHCP relay. This means that the Switch forwards all DHCP requests from all domains to the same DHCP server. You can also configure the Switch to relay DHCP information based on the VLAN membership of the DHCP clients.

34.3.1 DHCP Relay Agent Information

The Switch can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field to the **Option 82** field. The **Option 82** field is in the DHCP headers of client DHCP request frames that the Switch relays to a DHCP server.

Relay Agent Information can include the **System Name** of the Switch if you select this option. You can change the **System Name** in **Basic Settings** > **General Setup**.

The following describes the DHCP relay information that the Switch sends to the DHCP server:

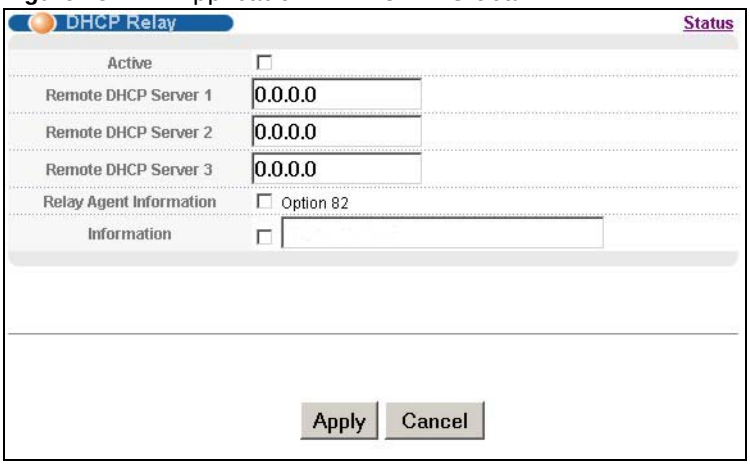
Table 122 Relay Agent Information

FIELD LABELS	DESCRIPTION
Slot ID	(1 byte) This value is always 0 for stand-alone switches.
Port ID	(1 byte) This is the port that the DHCP client is connected to.
VLAN ID	(2 bytes) This is the VLAN that the port belongs to.
Information	(up to 64 bytes) This optional, read-only field is set according to system name set in **Basic Settings > General Setup.**

34.3.2 Configuring DHCP Global Relay

Configure global DHCP relay in the **DHCP Relay** screen. Click **IP Application > DHCP** in the navigation panel and click the **Global** link to display the screen as shown.

Figure 154 IP Application > DHCP > Global



The following table describes the labels in this screen.

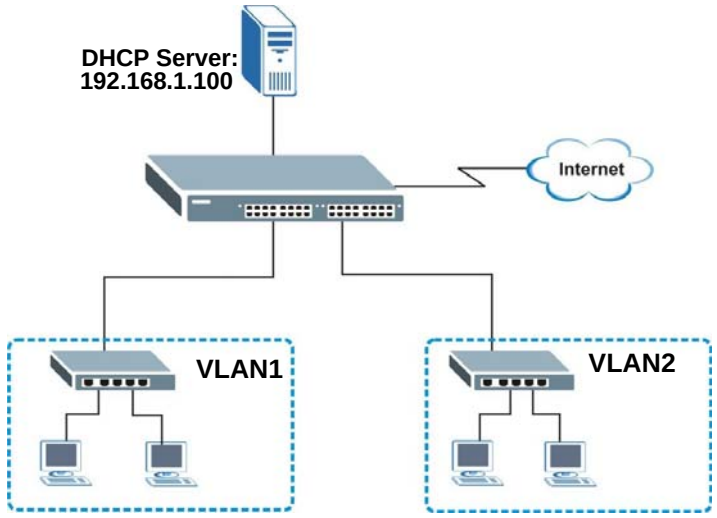
Table 123 IP Application > DHCP > Global

LABEL	DESCRIPTION
Active	Select this check box to enable DHCP relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the **Option 82** check box to have the Switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the **General Setup** screen. Select the check box for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

34.3.3 Global DHCP Relay Configuration Example

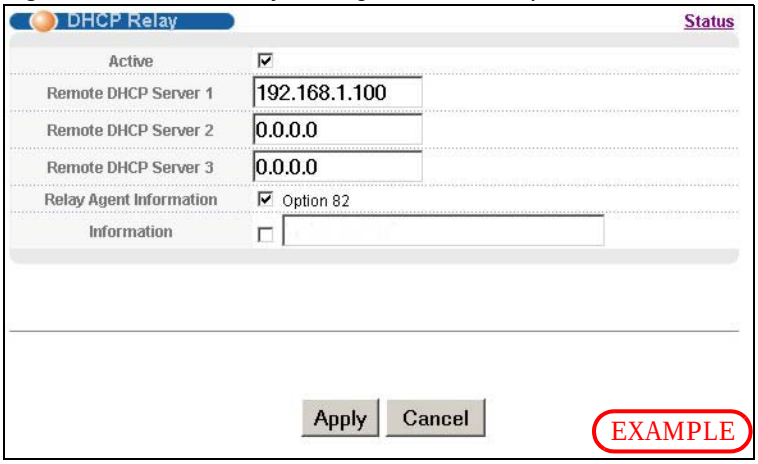
The follow figure shows a network example where the Switch is used to relay DHCP requests for the **VLAN1** and **VLAN2** domains. There is only one DHCP server that services the DHCP clients in both domains.

Figure 155 Global DHCP Relay Network Example



Configure the **DHCP Relay** screen as shown. Make sure you select the **Option 82** check box to set the Switch to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID.

Figure 156 DHCP Relay Configuration Example

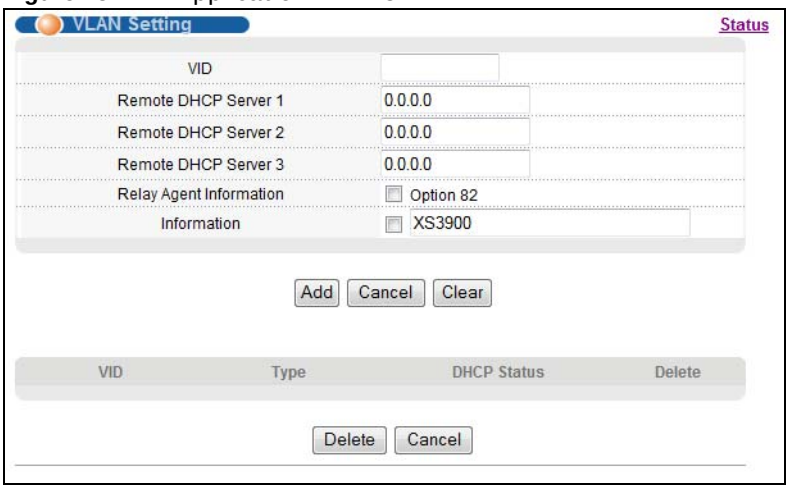


34.4 Configuring DHCP VLAN Settings

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **IP Application** > **DHCP** in the navigation panel, then click the **VLAN** link In the **DHCP Status** screen that displays.

Note: You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the Switch. See Section 6.6 on page 76 for information on how to do this.

Figure 157 IP Application > DHCP > VLAN



The following table describes the labels in this screen.

Table 124 IP Application > DHCP > VLAN

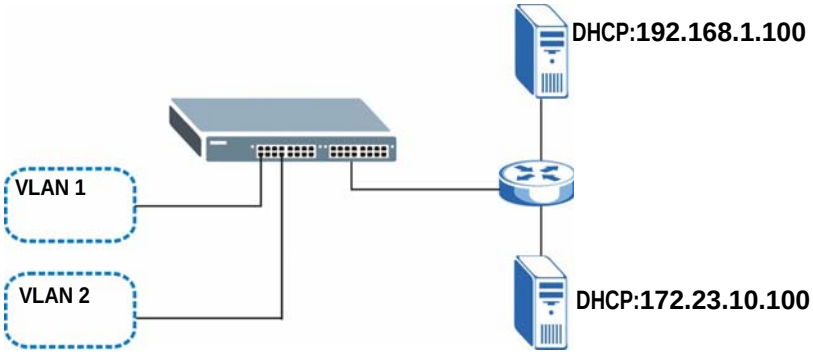
LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Relay Agent Information	Select the **Option 82** check box to have the Switch add information (slot number, port number and VLAN ID) to client DHCP requests that it relays to a DHCP server.
Information	This read-only field displays the system name you configure in the **General Setup** screen. Select the check box for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to reset the fields to the factory defaults.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays **Server** or **Relay** for the DHCP mode.
DHCP Status	For DHCP relay configuration, this field displays the first remote DHCP server IP address.
Delete	Select the configuration entries you want to remove and click **Delete** to remove them.
Cancel	Click **Cancel** to clear the **Delete** check boxes.

34.4.1 Example: DHCP Relay for Two VLANs

The following example displays two VLANs (VIDs 1 and 2) for a campus network. Two DHCP servers are installed to serve each VLAN. The system is set up to forward DHCP requests from the dormitory rooms (VLAN 1) to the DHCP server with an IP address of 192.168.1.100. Requests from

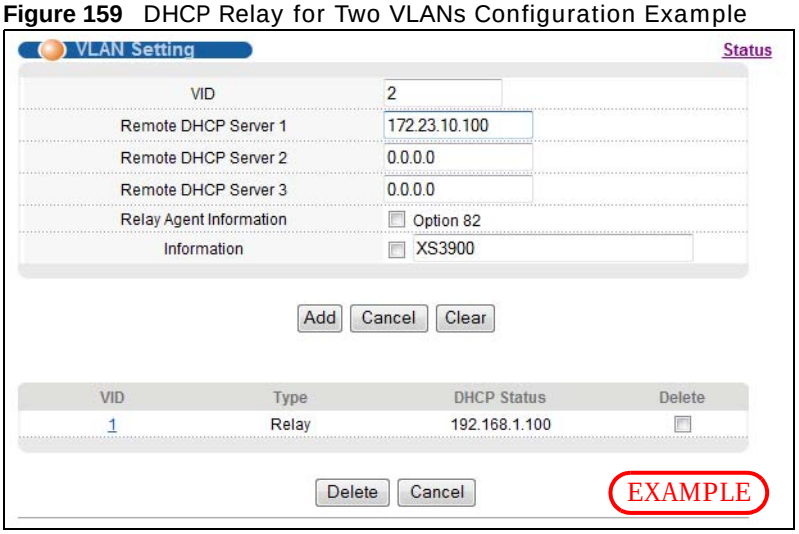
the academic buildings (VLAN 2) are sent to the other DHCP server with an IP address of 172.23.10.100.

Figure 158 DHCP Relay for Two VLANs



For the example network, configure the **VLAN Setting** screen as shown.

Figure 159 DHCP Relay for Two VLANs Configuration Example



35

Maintenance

This chapter explains how to configure the maintenance screens that let you maintain the firmware and configuration files.

35.1 The Maintenance Screen

Use this screen to manage firmware and your configuration files. Click **Management** > **Maintenance** in the navigation panel to open the following screen.

Figure 160 Management > Maintenance

The following table describes the labels in this screen.

Table 125 Management > Maintenance

LABEL	DESCRIPTION
Current	This field displays which configuration (**Configuration 1** or **Configuration 2**) is currently operating on the Switch.
Firmware Upgrade	Click **Click Here** to go to the **Firmware Upgrade** screen.
Restore Configuration	Click **Click Here** to go to the **Restore Configuration** screen.
Backup Configuration	Click **Click Here** to go to the **Backup Configuration** screen.
Load Factory Default	Click **Click Here** to reset the configuration to the factory default settings.
Save Configuration	Click **Config 1** to save the current configuration settings to **Configuration 1** on the Switch. Click **Config 2** to save the current configuration settings to **Configuration 2** on the Switch.
Reboot System	Click **Config 1** to reboot the system and load **Configuration 1** on the Switch. Click **Config 2** to reboot the system and load **Configuration 2** on the Switch. Note: Make sure to click the **Save** button in any screen to save your settings to the current configuration on the Switch.

35.2 Load Factory Default

Follow the steps below to reset the Switch back to the factory defaults.

1 In the **Maintenance** screen, click the **Click Here** button next to **Load Factory Default** to clear all Switch configuration information you configured and return to the factory defaults.

2 Click **OK** to reset all Switch configurations to the factory defaults.

Figure 161 Load Factory Default: Start

3 In the web configurator, click the **Save** button to make the changes take effect. If you want to access the Switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1).

35.3 Save Configuration

Click **Config 1** to save the current configuration settings permanently to configuration one on the Switch.

Click **Config 2** to save the current configuration settings to configuration two on the Switch.

Alternatively, click **Save** on the top right-hand corner in any screen to save the configuration changes to the current configuration.

Note: Clicking the **Apply** or **Add** button does NOT save the changes permanently. All unsaved changes are erased after you reboot the Switch.

35.4 Reboot System

Reboot System allows you to restart the Switch without physically turning the power off. It also allows you to load configuration one (**Config 1**) or configuration two (**Config 2**) when you reboot. Follow the steps below to reboot the Switch.

1 In the **Maintenance** screen, click the **Config 1** button next to **Reboot System** to reboot and load configuration one. The following screen displays.

Figure 162 Reboot System: Confirmation

2 Click **OK** again and then wait for the Switch to restart. This takes up to two minutes. This does not affect the Switch's configuration.

Click **Config 2** and follow steps 1 to 2 to reboot and load configuration two on the Switch.

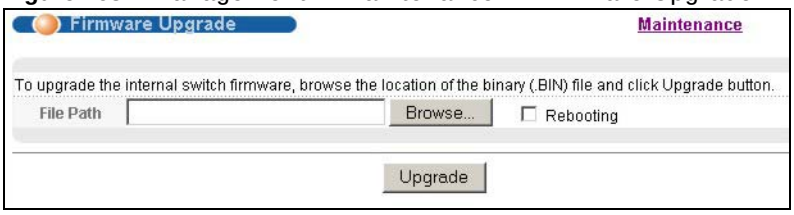
35.5 Firmware Upgrade

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

From the **Maintenance** screen, display the **Firmware Upgrade** screen as shown next.

Figure 163 Management > Maintenance > Firmware Upgrade



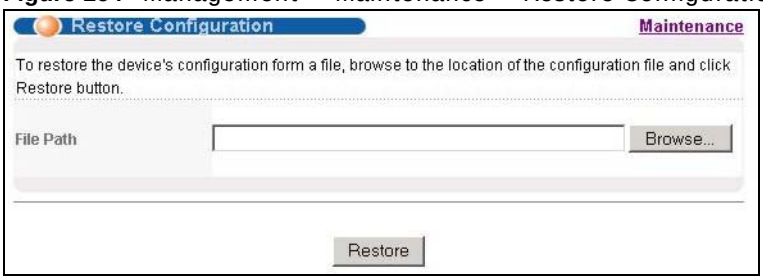
Type the path and file name of the firmware file you wish to upload to the Switch in the **File Path** text box or click **Browse** to locate it. Select the **Rebooting** checkbox if you want to reboot the Switch and apply the new firmware immediately. (Firmware upgrades are only applied after a reboot). Click **Upgrade** to load the new firmware.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

35.6 Restore a Configuration File

Restore a previously saved configuration from your computer to the Switch using the **Restore Configuration** screen.

Figure 164 Management > Maintenance > Restore Configuration


Restore Configuration
Maintenance
To restore the device's configuration form a file, browse to the location of the configuration file and click Restore button.
File Path
Browse...
Restore

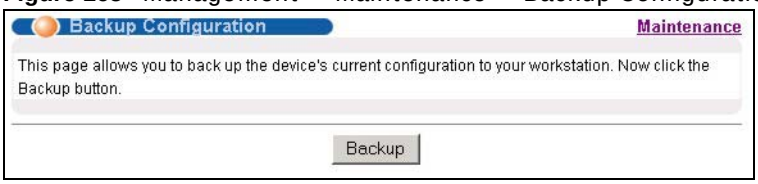
Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen from which you can locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.

35.7 Backup a Configuration File

Backing up your Switch configurations allows you to create various “snapshots” of your device from which you may restore at a later date.

Back up your current Switch configuration to a computer using the **Backup Configuration** screen.

Figure 165 Management > Maintenance > Backup Configuration


Backup Configuration
Maintenance
This page allows you to back up the device's current configuration to your workstation. Now click the Backup button.
Backup

Follow the steps below to back up the current Switch configuration to your computer in this screen.

1 Click **Backup**.

2 Click **Save** to display the **Save As** screen.

3 Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

35.8 FTP Command Line

This section shows some examples of uploading to or downloading files from the Switch using FTP commands. First, understand the filename conventions.

35.8.1 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the factory default settings in the screens such as password, Switch setup, IP Setup, and so on. Once you have customized the Switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System, sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension.

Table 126 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config	.cfg	This is the configuration (config) filename on the Switch. Uploading the config file replaces the specified configuration file system, including your Switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras-0 ras-1	*.bin	This is the generic name for the ZyNOS firmware on the Switch. `ras-0` is image 1; `ras-1` is image 2.

You can store up to two images, or firmware files of the same device model, on the Switch. Only one image is used at a time.

- Run the `boot image <1|2>` command to specify which image is updated when firmware is loaded using the web configurator and to specify which image is loaded when the Switch starts up.
- You can also use FTP commands to upload firmware to any image.

The Switch supports dual firmware images, `ras-0` and `ras-1`. You can switch from one to the other by using the `boot image <index>` command, where `<index>` is 1 (ras-0) or 2 (ras-1). See the CLI Reference Guide for more information about using commands. The system does not reboot after it switches from one image to the other.

35.8.1.1 Example FTP Commands

```
ftp> put firmware.bin ras-0
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the Switch.

```
ftp> get config config.cfg
```

This is a sample FTP session saving the current configuration to a file called "config.cfg" on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Switch only recognizes "config", "ras-0", and "ras-1". Be sure you keep unaltered copies of both files for later use.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

35.8.2 FTP Command Line Procedure

1. Launch the FTP client on your computer.
2. Enter open, followed by a space and the IP address of your Switch.
3. Press [ENTER] when prompted for a username (the default is “admin”).
4. Enter your password as requested (the default is “1234”).
5. Enter `bin` to set transfer mode to binary.
6. Use `put` to transfer files from the computer to the Switch, for example, `put firmware.bin ras-0` transfers the firmware on your computer (firmware.bin) to the Switch and renames it to “ras-0”. Similarly, `put config.cfg config` transfers the configuration file on your computer (config.cfg) to the Switch and renames it to “config”. Likewise `get config config.cfg` transfers the configuration file on the Switch to your computer and renames it to “config.cfg”. See Table 126 on page 273 for more information on filename conventions.
7. Enter `quit` to exit the ftp prompt.

35.8.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 127 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

35.8.4 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Service Access Control** screen.

- The IP address(es) in the **Remote Management** screen does not match the client IP address. If it does not match, the Switch will disconnect the FTP session immediately.

36

Access Control

This chapter describes how to control access to the Switch.

36.1 Access Control Overview

A console port and FTP are allowed one session each, Telnet and SSH share nine sessions, up to five Web sessions (five different usernames and passwords) and/or limitless SNMP access control sessions are allowed.

Table 128 Access Control Overview

Console Port	SSH	Telnet	FTP	Web	SNMP
One session	Share up to nine sessions		One session	Up to five accounts	No limit

A console port access control session and Telnet access control session cannot coexist when multi-login is disabled. See the Ethernet Switch CLI Reference Guide for more information on disabling multi-login.

36.2 The Access Control Main Screen

Click **Management > Access Control** in the navigation panel to display the main screen as shown.

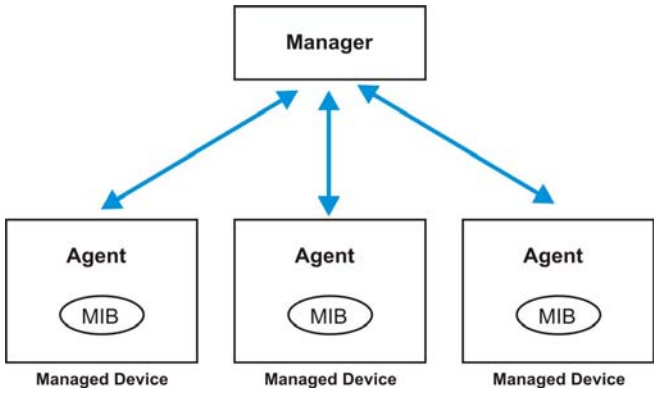
Figure 166 Management > Access Control

36.3 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network via SNMP version 1 (SNMPv1), SNMP version 2c or

SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 167 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed Switch (the Switch). An agent translates the local management information from the managed Switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a Switch. Examples of variables include number of packets received, node port status and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 129 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

36.3.1 SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

36.3.2 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The Switch supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIBs
- RFC 1643 Ethernet MIBs
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP

36.3.3 SNMP Traps

The Switch sends traps to an SNMP manager when an event occurs. The following tables outline the SNMP traps by category.

An OID (Object ID) that begins with "**1.3.6.1.4.1.890.1.5.8**" is defined in private MIBs. Otherwise, it is a standard MIB OID.

Note: The OIDs beginning with "1.3.6.1.4.1.890.1.5.8.74" are specific to the XS3900-48F switch.

Table 130 SNMP System Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
coldstart	coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent when the Switch is turned on.
warmstart	warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the Switch restarts.
fanspeed	FanSpeedEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when the fan speed goes above or below the normal operating range.
	FanSpeedEventClear	1.3.6.1.4.1.890.1.5.8.74.31.2.2	This trap is sent when the fan speed returns to the normal operating range.
temperature	TemperatureEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when the temperature goes above or below the normal operating range.
	TemperatureEventClear	1.3.6.1.4.1.890.1.5.8.74.31.2.2	This trap is sent when the temperature returns to the normal operating range.
voltage	VoltageEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when the voltage goes above or below the normal operating range.
	VoltageEventClear	1.3.6.1.4.1.890.1.5.8.74.31.2.2	This trap is sent when the voltage returns to the normal operating range.

Table 130 SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
fanairflow	FanAirFlowEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	Fan module and power module fan air-flow must be in the same direction (front-to-back or back-to-front) on the same Switch. This trap is sent when the airflows are not in the same direction.
	FanAirFlowEventClear	1.3.6.1.4.1.890.1.5.8.74.31.2.2	Fan module and power module fan air-flow must be in the same direction (front-to-back or back-to-front) on the same Switch. This trap is sent when the airflows return to the same direction.
reset	UncontrolledResetEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when the Switch automatically resets.
	ControlledResetEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when the Switch resets by an administrator through a management interface.
	RebootEvent	1.3.6.1.4.1.890.1.5.1.1.2	This trap is sent when the Switch reboots by an administrator through a management interface.
timesync	RTCNotUpdatedEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when the Switch fails to get the time and date from a time server.
	RTCNotUpdatedEventClear	1.3.6.1.4.1.890.1.5.8.74.31.2.2	This trap is sent when the Switch gets the time and date from a time server.
intrusionlock	IntrusionLockEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when intrusion lock occurs on a port.
loopguard	LoopguardEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when loopguard shuts down a port.
errdisable	errdisableDetect	1.3.6.1.4.1.890.1.5.8.74.130.4.1	This trap is sent when an error is detected on a port, such as a loop occurs or the rate limit for specific control packets is exceeded.
	errdisableRecovery	1.3.6.1.4.1.890.1.5.8.74.130.4.2	This trap is sent when the Switch ceases the action taken on a port, such as shutting down the port or discarding packets on the port, after the specified recovery interval.

Table 131 SNMP InterfaceTraps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
	LinkDownEventClear	1.3.6.1.4.1.890.1.5.8.74.31.2.2	This trap is sent when the Ethernet link is up.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
	LinkDownEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when the Ethernet link is down.

Table 131 SNMP InterfaceTraps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
autonegotiation	AutonegotiationFailedEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when an Ethernet interface fails to auto-negotiate with the peer Ethernet interface.
	AutonegotiationFailedEventClear	1.3.6.1.4.1.890.1.5.8.74.31.2.2	This trap is sent when an Ethernet interface auto-negotiates with the peer Ethernet interface.
lldp	lldpRemTablesChange	1.0.8802.1.1.2.0.0.1	The trap is sent when entries in the remote database have any updates. Link Layer Discovery Protocol (LLDP), defined as IEEE 802.1ab, enables LAN devices that support LLDP to exchange their configured settings. This helps eliminate configuration mismatch issues.
transceiver-ddm	DDMIRxPowerEventOn DDMITemperatureEventOn DDMITxBiasEventOn DDMITxPowerEventOn DDMIVoltageEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when one of the device operating parameters (such as transceiver temperature, laser bias current, transmitted optical power, received optical power and transceiver supply voltage) is above or below a factory set normal range.
	DDMIRxPowerEventClear DDMITemperatureEventClear DDMITxBiasEventClear DDMITxPowerEventClear DDMIVoltageEventClear	1.3.6.1.4.1.890.1.5.8.74.31.2.2	This trap is sent when all device operating parameters return to the normal operating range.

Table 132 AAA Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
authentication	authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when authentication fails due to incorrect user name and/or password.
	AuthenticationFailureEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when authentication fails due to incorrect user name and/or password.
	RADIUSNotReachableEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when there is no response message from the RADIUS server.
	RADIUSNotReachableEventClear	1.3.6.1.4.1.890.1.5.8.74.31.2.2	This trap is sent when the RADIUS server can be reached.

Table 132 AAA Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
accounting	RADIUSAcctNotReachableEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when there is no response message from the RADIUS accounting server.
	RADIUSAcctNotReachableEventClear	1.3.6.1.4.1.890.1.5.8.74.31.2.2	This trap is sent when the RADIUS accounting server can be reached.

Table 133 SNMP IP Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
ping	pingProbeFailed	1.3.6.1.2.1.80.0.1	This trap is sent when a single ping probe fails.
	pingTestFailed	1.3.6.1.2.1.80.0.2	This trap is sent when a ping test (consisting of a series of ping probes) fails.
	pingTestCompleted	1.3.6.1.2.1.80.0.3	This trap is sent when a ping test is completed.
traceroute	traceRouteTestFailed	1.3.6.1.2.1.81.0.2	This trap is sent when a traceroute test fails.
	traceRouteTestCompleted	1.3.6.1.2.1.81.0.3	This trap is sent when a traceroute test is completed.

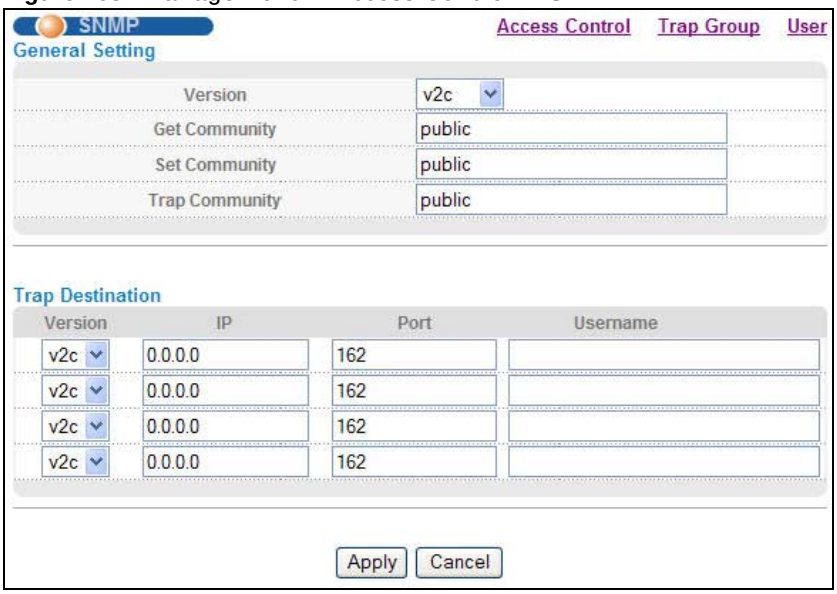
Table 134 SNMP Switch Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
stp	STPNewRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP root switch changes.
	MRSTPNewRoot	1.3.6.1.4.1.890.1.5.8.74.35.2.1	This trap is sent when the MRSTP root switch changes.
	MSTPNewRoot	1.3.6.1.4.1.890.1.5.8.74.107.70.1	This trap is sent when the MSTP root switch changes.
	STPTopologyChange	1.3.6.1.2.1.17.0.2	This trap is sent when the STP topology changes.
	MRSTPTopologyChange	1.3.6.1.4.1.890.1.5.8.74.35.2.2	This trap is sent when the MRSTP topology changes.
	MSTPTopologyChange	1.3.6.1.4.1.890.1.5.8.74.107.70.2	This trap is sent when the MSTP root switch changes.
mactable	MacTableFullEventOn	1.3.6.1.4.1.890.1.5.8.74.31.2.1	This trap is sent when more than 99% of the MAC table is used.
	MacTableFullEventClear	1.3.6.1.4.1.890.1.5.8.74.31.2.2	This trap is sent when less than 95% of the MAC table is used.
rmon	RmonRisingAlarm	1.3.6.1.2.1.16.0.1	This trap is sent when a variable goes over the RMON "rising" threshold.
	RmonFallingAlarm	1.3.6.1.2.1.16.0.2	This trap is sent when the variable falls below the RMON "falling" threshold.
cfm	dot1agCfmFaultAlarm	1.3.111.2.802.1.1.8.0.1	The trap is sent when the Switch detects a connectivity fault.

36.3.4 Configuring SNMP

From the **Access Control** screen, display the **SNMP** screen. You can click **Access Control** to go back to the **Access Control** screen.

Figure 168 Management > Access Control > SNMP



The following table describes the labels in this screen.

Table 135 Management > Access Control > SNMP

LABEL	DESCRIPTION
General Setting	Use this section to specify the SNMP version and community (password) values.
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (**v2c**), SNMP version 3 (**v3**) or both (**v3v2c**). Note: SNMP version 2c is backwards compatible with SNMP version 1.
Get Community	Enter the **Get Community** string, which is the password for the incoming Get- and GetNext- requests from the management station. The **Get Community** string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the **Set Community** string, which is the password for the incoming Set- requests from the management station. The **Set Community** string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the **Trap Community** string, which is the password sent with each trap to the SNMP manager. The **Trap Community** string is only used by SNMP managers using SNMP version 2c or lower.
Trap Destination	Use this section to configure where to send SNMP traps from the Switch.
Version	Specify the version of the SNMP trap messages.
IP	Enter the IP addresses of up to four managers to send your SNMP traps to.
Port	Enter the port number upon which the manager listens for SNMP traps.

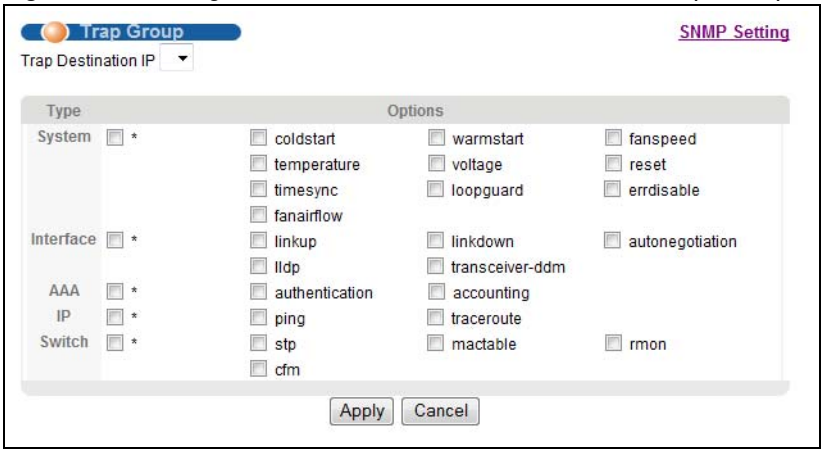
Table 135 Management > Access Control > SNMP (continued)

LABEL	DESCRIPTION
Username	Enter the username to be sent to the SNMP manager along with the SNMP v3 trap. Note: This username must match an existing account on the Switch (configured in the **Management > Access Control > SNMP > User** screen).
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

36.3.5 Configuring SNMP Trap Group

From the **SNMP** screen, click **Trap Group** to view the screen as shown. Use the **Trap Group** screen to specify the types of SNMP traps that should be sent to each SNMP manager.

Figure 169 Management > Access Control > SNMP > Trap Group



The following table describes the labels in this screen.

Table 136 Management > Access Control > SNMP > Trap Group

LABEL	DESCRIPTION
Trap Destination IP	Select one of your configured trap destination IP addresses. These are the IP addresses of the SNMP managers. You must first configure a trap destination IP address in the **SNMP Setting** screen. Use the rest of the screen to select which traps the Switch sends to that SNMP manager.
Type	Select the categories of SNMP traps that the Switch is to send to the SNMP manager.
Options	Select the individual SNMP traps that the Switch is to send to the SNMP station. See Section 36.3.3 on page 278 for individual trap descriptions. The traps are grouped by category. Selecting a category automatically selects all of the category's traps. Clear the check boxes for individual traps that you do not want the Switch to send to the SNMP station. Clearing a category's check box automatically clears all of the category's trap check boxes (the Switch only sends traps from selected categories).

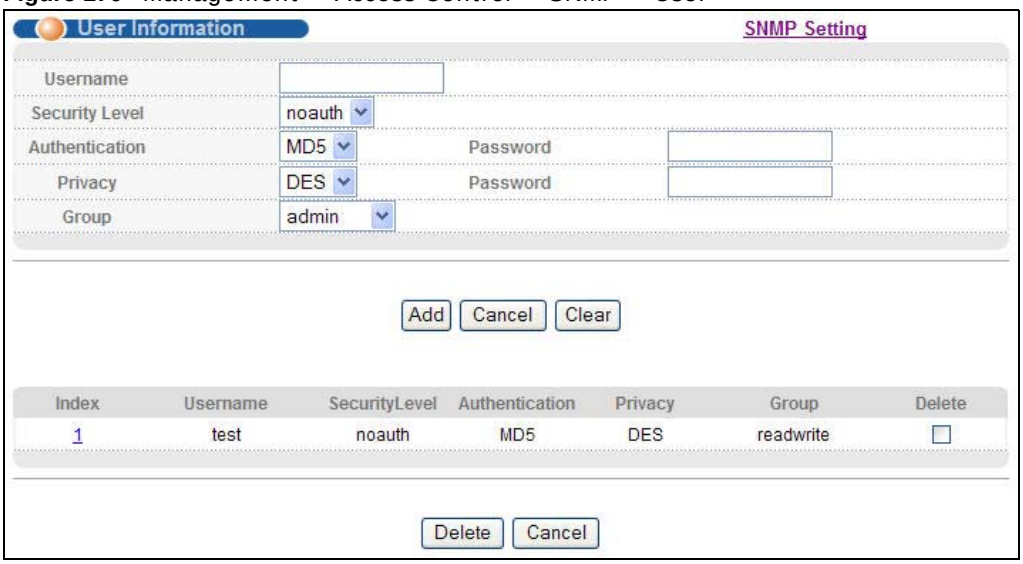
Table 136 Management > Access Control > SNMP > Trap Group (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

36.3.6 Configuring SNMP User

From the **SNMP** screen, click **User** to view the screen as shown. Use the **User** screen to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups. An SNMP user is an SNMP manager.

Figure 170 Management > Access Control > SNMP > User



The following table describes the labels in this screen.

Table 137 Management > Access Control > SNMP > User

LABEL	DESCRIPTION
User Information	Note: Use the username and password of the login accounts you specify in this screen to create accounts on the SNMP v3 manager.
Username	Specify the username of a login account on the Switch.
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: • **noauth** -to use the username as the password string to send to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level. • **auth** - to implement an authentication algorithm for SNMP messages sent by this user. • **priv** - to implement authentication and encryption for SNMP messages sent by this user. This is the highest security level. Note: The settings on the SNMP manager must be set at the same security level or higher than the security level settings on the Switch.

Table 137 Management > Access Control > SNMP > User (continued)

LABEL	DESCRIPTION
Authentication	Select an authentication algorithm. **MD5** (Message Digest 5) and **SHA** (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Password	Enter the password of up to 32 ASCII characters for SNMP user authentication.
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: • **DES** - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • **AES** - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Password	Enter the password of up to 32 ASCII characters for encrypting SNMP packets.
Group	SNMP v3 adopts the concept of View-based Access Control Model (VACM) group. SNMP managers in one group are assigned common access rights to MIBs. Specify in which SNMP group this user is. **admin** - Members of this group can perform all types of system configuration, including the management of administrator accounts. **readwrite** - Members of this group have read and write rights, meaning that the user can create and edit the MIBs on the Switch, except the user account and AAA configuration. **readonly** - Members of this group have read rights only, meaning the user can collect information from the Switch.
Add	Click **Add** to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
Clear	Click **Clear** to reset the fields to the factory defaults.
Index	This is a read-only number identifying a login account on the Switch. Click on an index number to view more details and edit an existing account.
Username	This field displays the username of a login account on the Switch.
Security Level	This field displays whether you want to implement authentication and/or encryption for SNMP communication with this user.
Authentication	This field displays the authentication algorithm used for SNMP communication with this user.
Privacy	This field displays the encryption method used for SNMP communication with this user.
Group	This field displays the SNMP group to which this user belongs.
Delete	Click **Delete** to remove the selected entry from the summary table.
Cancel	Click **Cancel** to begin configuring this screen afresh.

36.4 Setting Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the Switch via web configurator at any one time.

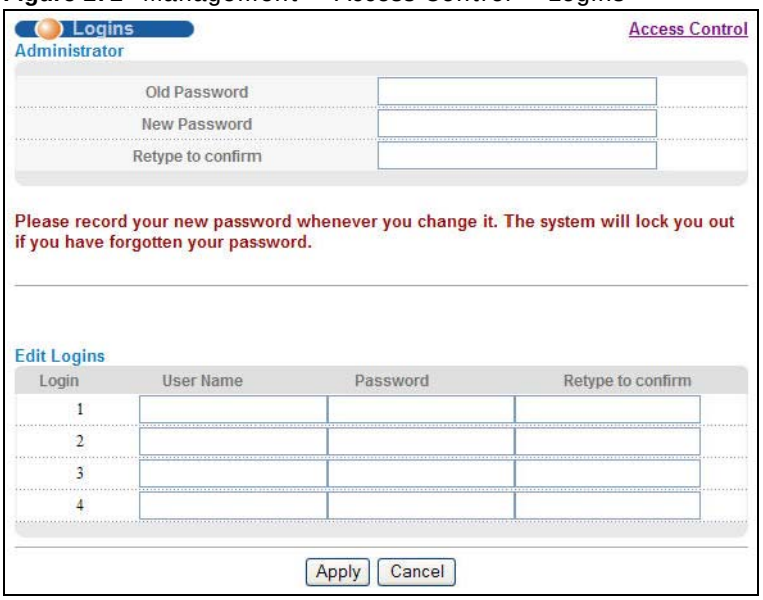
- An administrator is someone who can both view and configure Switch changes. The username for the Administrator is always **admin**. The default administrator password is **1234**.

Note: It is highly recommended that you change the default administrator password (**1234**).

- A non-administrator (username is something other than **admin**) is someone who can view but not configure Switch settings.

Click **Management > Access Control > Logins** to view the screen as shown.

Figure 171 Management > Access Control > Logins



The following table describes the labels in this screen.

Table 138 Management > Access Control > Logins

LABEL	DESCRIPTION
Administrator This is the default administrator account with the “admin” user name. You cannot change the default administrator user name. Only the administrator has read/write access.	
Old Password	Type the existing system password (**1234** is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Edit Logins You may configure passwords for up to four users. These users have read-only access. You can give users higher privileges via the CLI. For more information on assigning privileges see the Ethernet Switch CLI Reference Guide.	
User Name	Set a user name (up to 32 ASCII characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

36.5 Service Access Control Overview

This section introduces some of the services you can use to access and manage the Switch.

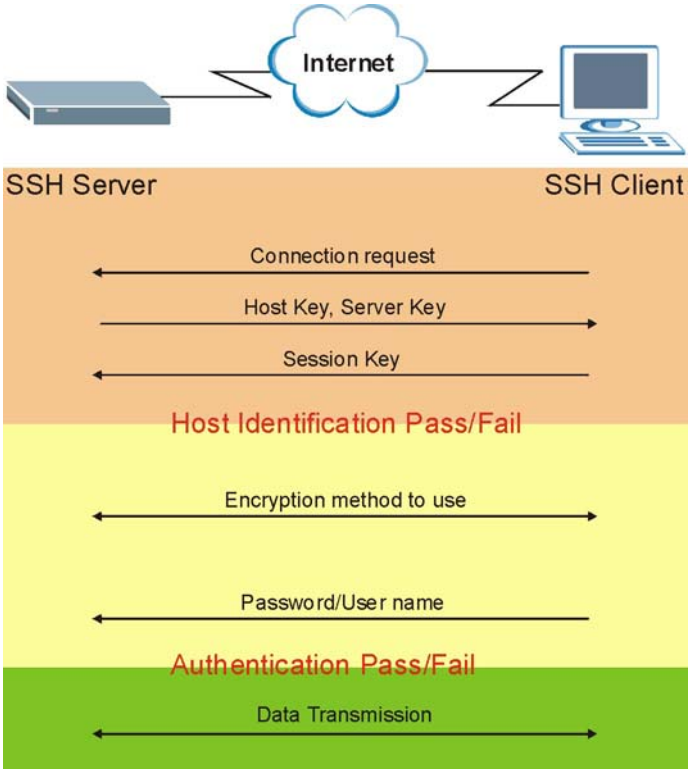
36.5.1 SSH

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Figure 172 SSH Communication Example

The following table summarizes how a secure connection is established between two remote hosts.

Figure 173 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

36.5.1.1 SSH Implementation on the Switch

Your Switch supports SSH version 2 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the Switch for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

36.5.1.2 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Switch over SSH.

36.5.2 HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys.

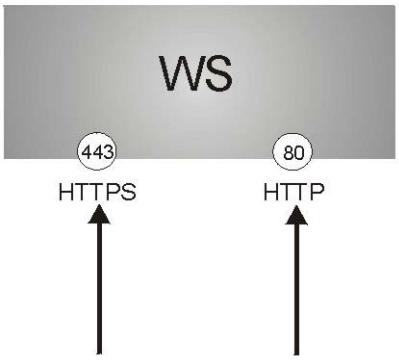
HTTPS on the Switch is used so that you may securely access the Switch using the web configurator. The SSL protocol specifies that the SSL server (the Switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Switch), whereas the SSL client only should authenticate itself when the SSL server requires it to do so. Authenticating client certificates is optional and if selected means the SSL-client must send the Switch a certificate. You must apply for a certificate for the browser from a Certificate Authority (CA) that is a trusted CA on the Switch.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Switch's WS (web server).

2 HTTP connection requests from a web browser go to port 80 (by default) on the Switch's WS (web server).

Figure 174 HTTPS Implementation



Note: If you disable **HTTP** in the **Service Access Control** screen, then the Switch blocks all HTTP connection attempts.

36.5.2.1 HTTPS Example

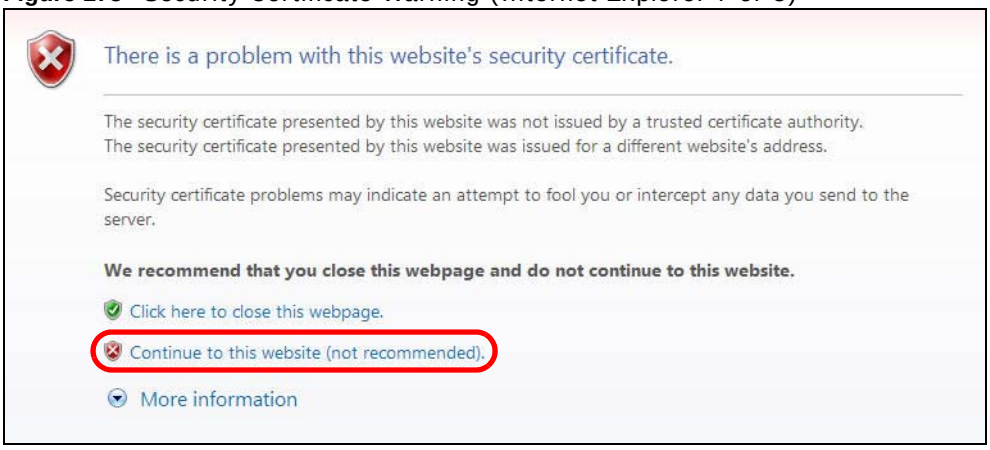
If you haven't changed the default HTTPS port on the Switch, then in your browser enter "https://Switch IP Address/" as the web site address where "Switch IP Address" is the IP address or domain name of the Switch you wish to access.

36.5.2.2 Internet Explorer Warning Messages

36.5.2.3 Internet Explorer 7 or 8

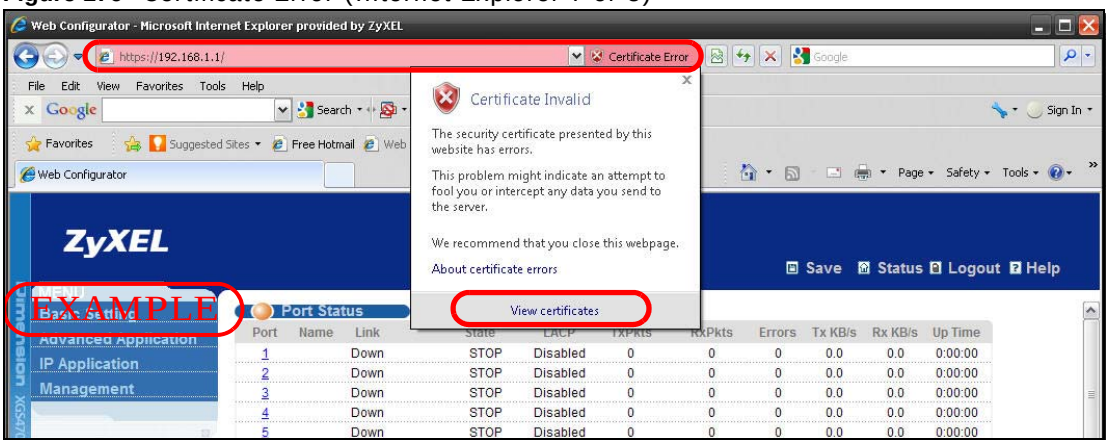
When you attempt to access the Switch HTTPS server, a screen with the message "There is a problem with this website's security certificate." may display. If that is the case, click **Continue to this website (not recommended)** to proceed to the web configurator login screen.

Figure 175 Security Certificate Warning (Internet Explorer 7 or 8)


There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

After you log in, you will see the red address bar with the message **Certificate Error**. Click on **Certificate Error** next to the address bar and click **View certificates**.

Figure 176 Certificate Error (Internet Explorer 7 or 8)



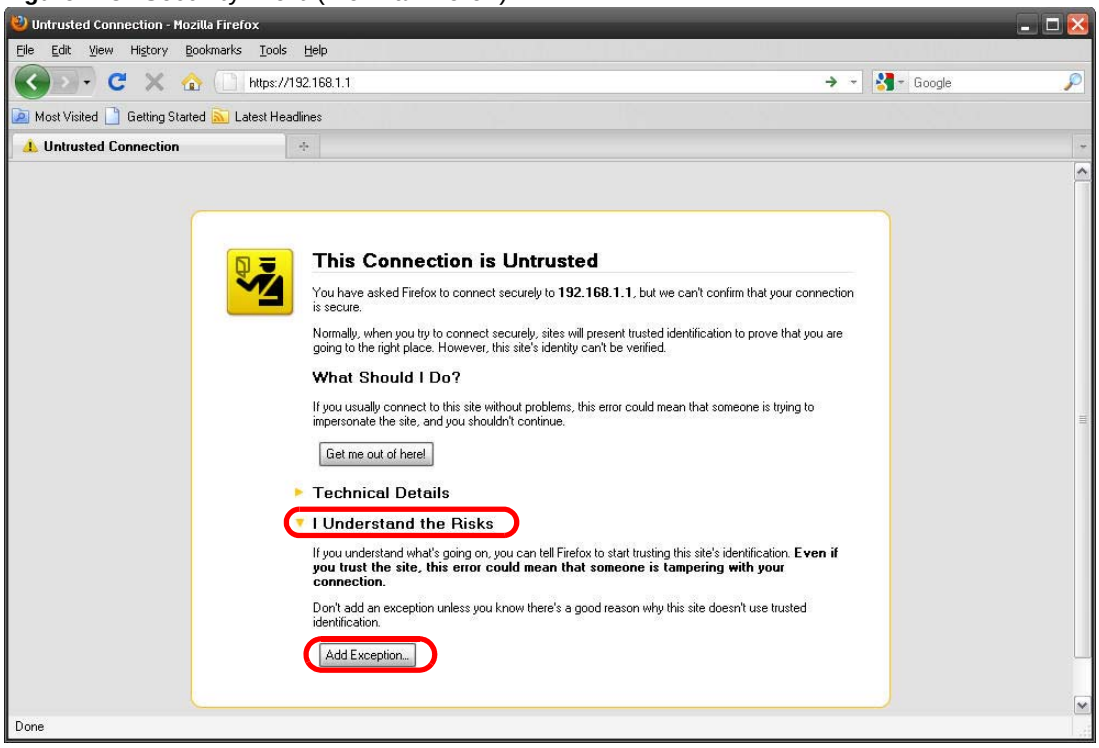
Click **Install Certificate...** and follow the on-screen instructions to install the certificate in your browser.

Figure 177 Certificate (Internet Explorer 7 or 8)

36.5.2.4 Mozilla Firefox Warning Messages

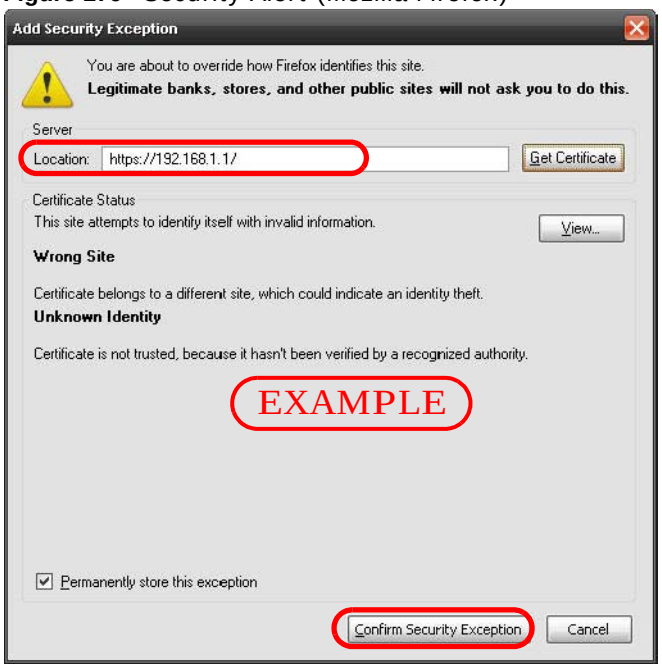
When you attempt to access the Switch HTTPS server, a **This Connection is Unstructed** screen may display. If that is the case, click **I Understand the Risks** and then the **Add Exception...** button.

Figure 178 Security Alert (Mozilla Firefox)


Untrusted Connection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://192.168.1.1
Google
Most Visited Getting Started Latest Headlines
Untrusted Connection
This Connection is Untrusted
You have asked Firefox to connect securely to 192.168.1.1, but we can't confirm that your connection is secure.
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.
What Should I Do?
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.
Get me out of here!
Technical Details
I Understand the Risks
If you understand what's going on, you can tell Firefox to start trusting this site's identification. Even if you trust the site, this error could mean that someone is tampering with your connection.
Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.
Add Exception...
Done

Confirm the HTTPS server URL matches. Click **Confirm Security Exception** to proceed to the web configurator login screen.

Figure 179 Security Alert (Mozilla Firefox)

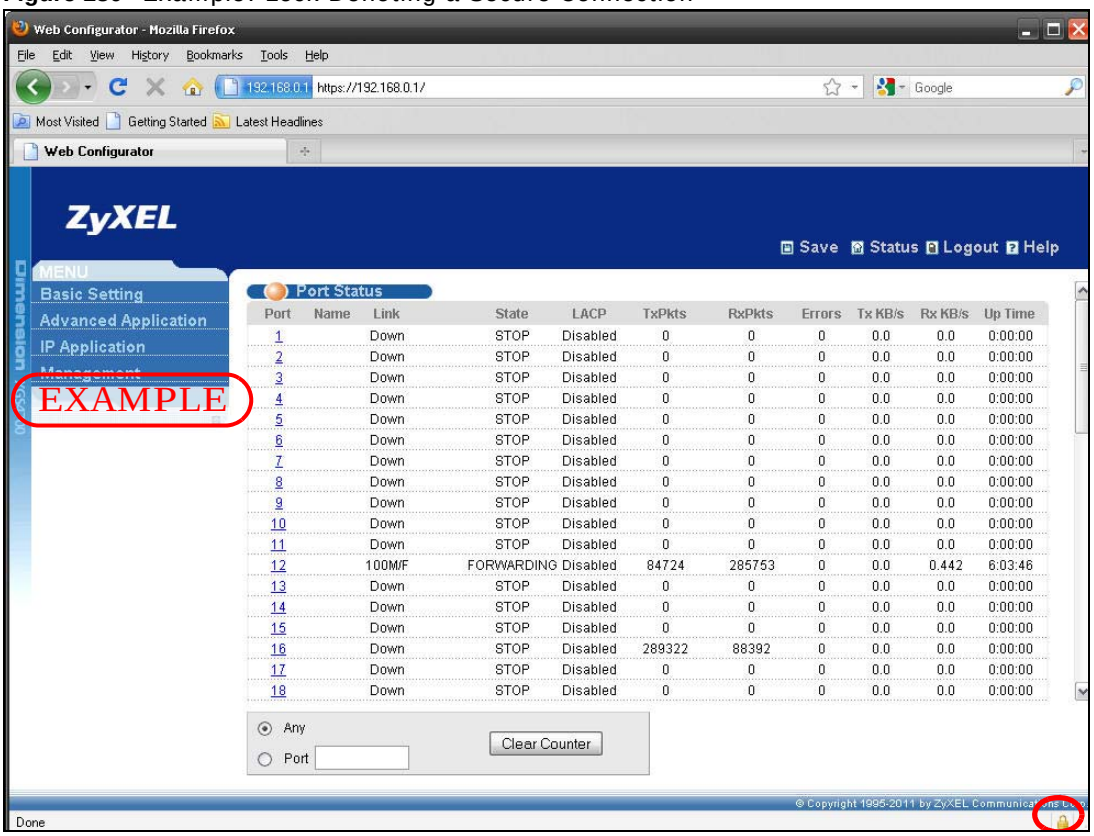

Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location: https://192.168.1.1/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View...
Wrong Site
Certificate belongs to a different site, which could indicate an identity theft.
Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority.
EXAMPLE
Permanently store this exception
Confirm Security Exception
Cancel

36.5.2.5 The Main Screen

After you accept the certificate and enter the login username and password, the Switch main screen appears. The lock displayed in the bottom right of the browser status bar (in Internet Explorer 6 or

Mozilla Firefox) or next to the address bar (in Internet Explorer 7 or 8) denotes a secure connection.

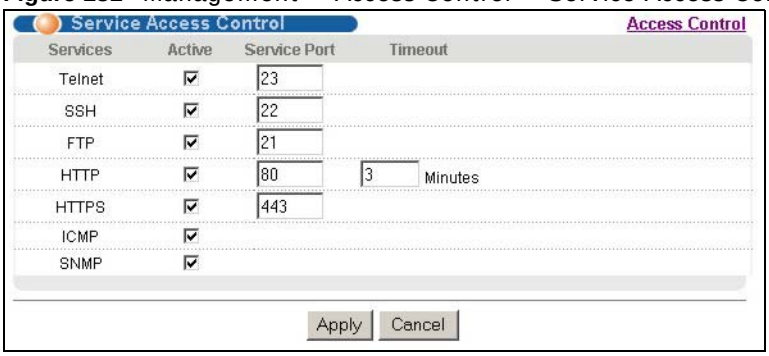
Figure 180 Example: Lock Denoting a Secure Connection


Web Configurator - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://192.168.0.1/
Most Visited Getting Started Latest Headlines
Web Configurator
ZyXEL
Save Status Logout Help
MENU
Basic Setting
Advanced Application
IP Application
EXAMPLE
Port Status
Port Name Link State LACP TxPkts RxPkts Errors Tx KB/s Rx KB/s Up Time
1 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
2 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
3 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
4 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
5 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
6 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
7 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
8 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
9 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
10 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
11 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
12 100M/F FORWARDING Disabled 84724 285753 0 0.0 0.442 6:03:46
13 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
14 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
15 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
16 Down STOP Disabled 289322 88392 0 0.0 0.0 0:00:00
17 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
18 Down STOP Disabled 0 0 0 0.0 0.0 0:00:00
Any
Port
Clear Counter
Done

36.5.3 Configuring Service Port Access Control

Service Access Control allows you to decide what services you may use to access the Switch. You may also change the default service port and configure “trusted computer(s)” for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the main **Access Control** screen.

Figure 181 Management > Access Control > Service Access Control



The following table describes the fields in this screen.

Table 139 Management > Access Control > Service Access Control

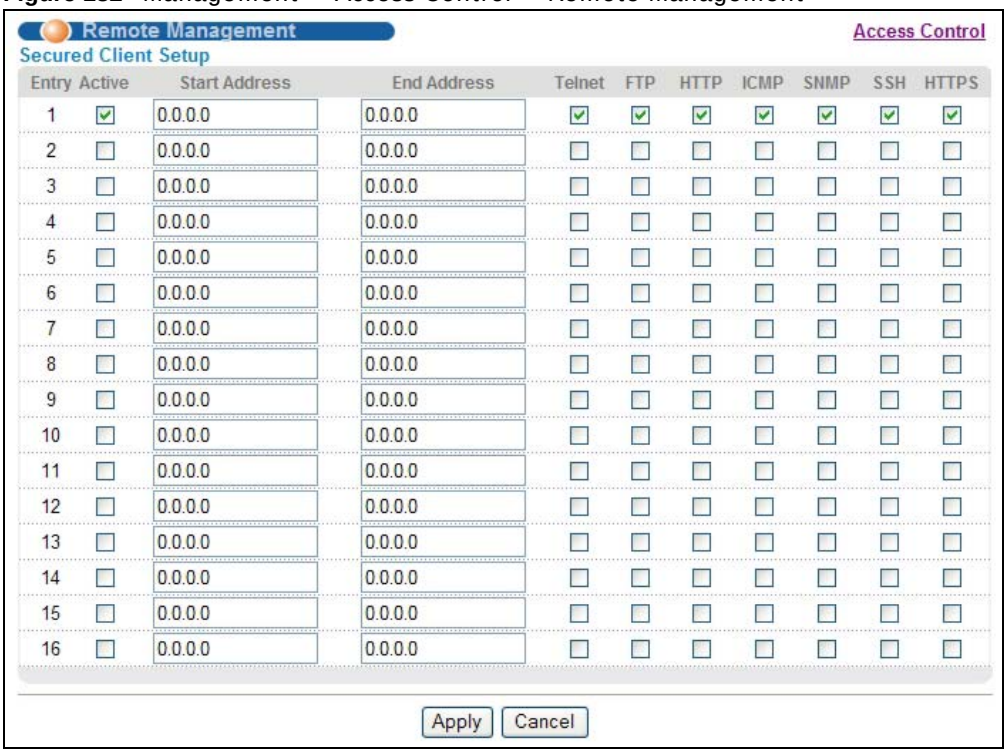
LABEL	DESCRIPTION
Services	Services you may use to access the Switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the Switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the **Server Port** field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Type how many minutes a management session (via the web configurator) can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

36.6 Remote Management

From the **Access Control** screen, display the **Remote Management** screen as shown next.

You can specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch. Click **Access Control** to return to the **Access Control** screen.

Figure 182 Management > Access Control > Remote Management



The following table describes the labels in this screen.

Table 140 Management > Access Control > Remote Management

LABEL	DESCRIPTION
Entry	This is the client set index number. A “client set” is a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IP address range of trusted computers from which you can manage this Switch. The Switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The Switch immediately disconnects the session if it does not match.
Telnet/FTP/HTTP/ICMP/ SNMP/SSH/HTTPS	Select services that may be used for managing the Switch from the specified trusted computers.
Apply	Click **Apply** to save your changes to the Switch’s run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

37

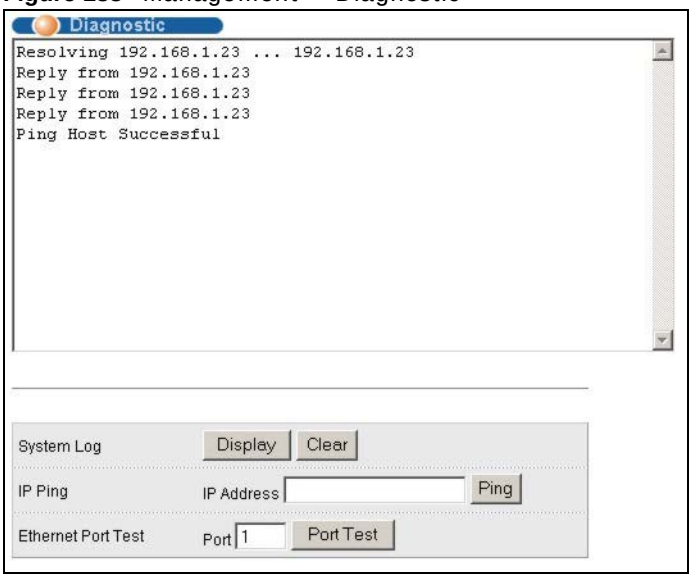
Diagnostic

This chapter explains the **Diagnostic** screen.

37.1 Diagnostic

Click **Management** > **Diagnostic** in the navigation panel to open this screen. Use this screen to check system logs, ping IP addresses or perform port tests.

Figure 183 Management > Diagnostic



The following table describes the labels in this screen.

Table 141 Management > Diagnostic

LABEL	DESCRIPTION
System Log	Click **Display** to display a log of events in the multi-line text box. Click **Clear** to empty the text box and reset the syslog entry.
IP Ping	Type the IP address of a device that you want to ping in order to test a connection. Click **Ping** to have the Switch ping the IP address (in the field to the left).
Ethernet Port Test	Enter a port number and click **Port Test** to perform an internal loopback test.

38

Syslog

This chapter explains the syslog screens.

38.1 Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

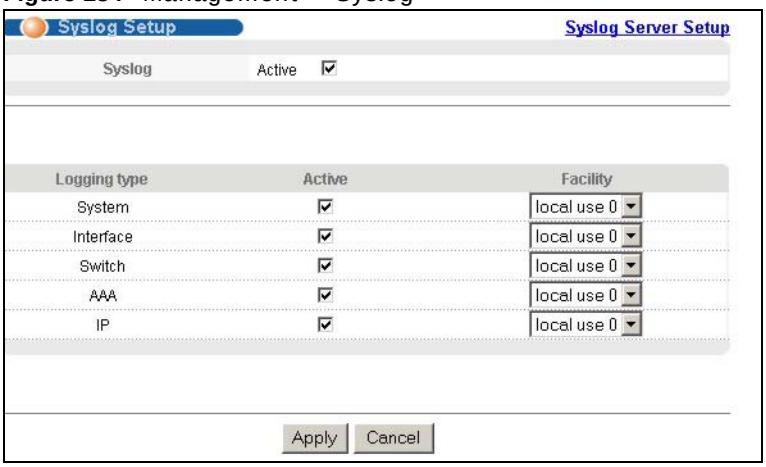
Table 142 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

38.2 Syslog Setup

Click **Management** > **Syslog** in the navigation panel to display this screen. The syslog feature sends logs to an external syslog server. Use this screen to configure the device's system logging settings.

Figure 184 Management > Syslog



The following table describes the labels in this screen.

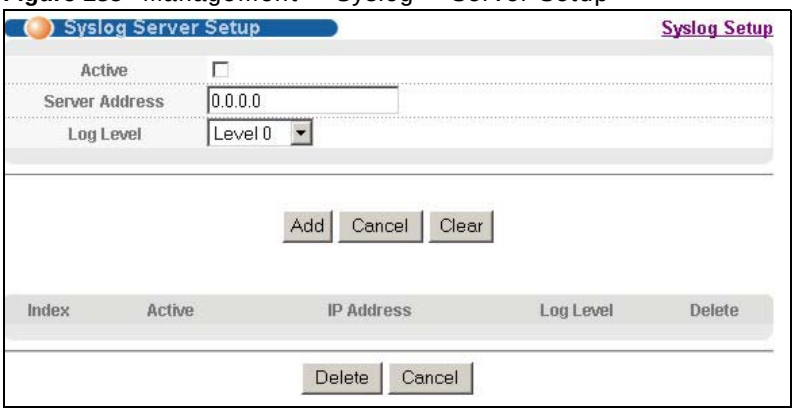
Table 143 Management > Syslog

LABEL	DESCRIPTION
Syslog	Select **Active** to turn on syslog (system logging) and then configure the syslog setting
Logging Type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

38.3 Syslog Server Setup

Click **Management** > **Syslog** > **Syslog Server Setup** to open the following screen. Use this screen to configure a list of external syslog servers.

Figure 185 Management > Syslog > Server Setup



The following table describes the labels in this screen.

Table 144 Management > Syslog > Server Setup

LABEL	DESCRIPTION
Active	Select this check box to have the device send logs to this syslog server. Clear the check box if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IP address of the syslog server.
Log Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clear	Click **Clear** to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays **Yes** if the device is to send logs to the syslog server. **No** displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Delete	Select an entry's **Delete** check box and click **Delete** to remove the entry.
Cancel	Click **Cancel** to begin configuring this screen afresh.

39

Cluster Management

This chapter introduces cluster management.

39.1 Clustering Management Status Overview

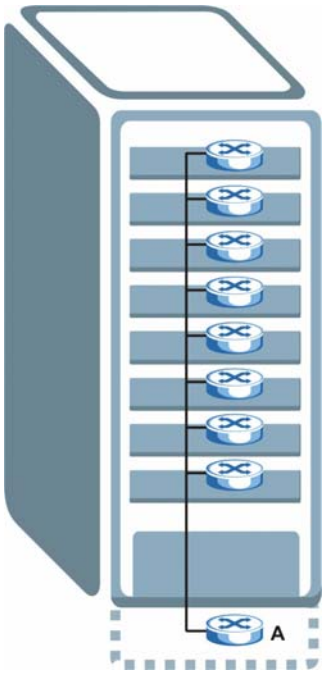
Cluster Management allows you to manage switches through one Switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 145 ZyXEL Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Cluster member models must be compatible with ZyXEL cluster management implementation.
Cluster Manager	The cluster manager is the Switch through which you manage the cluster member switches.
Cluster Members	Cluster members are the switches being managed by the cluster manager switch.

In the following example, switch **A** in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

Figure 186 Clustering Application Example

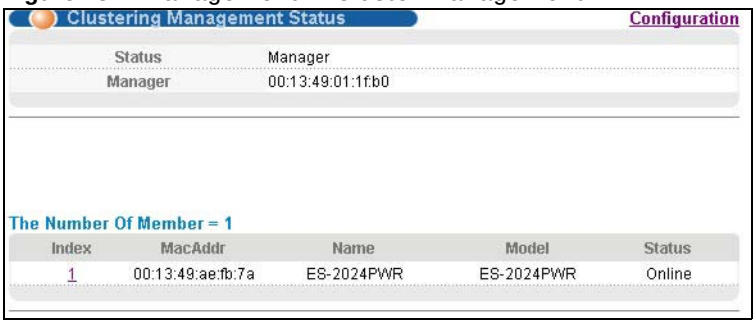


39.2 Cluster Management Status

Click **Management** > **Cluster Management** in the navigation panel to display the following screen.

Note: A cluster can only have one manager.

Figure 187 Management > Cluster Management



The following table describes the labels in this screen.

Table 146 Management > Cluster Management

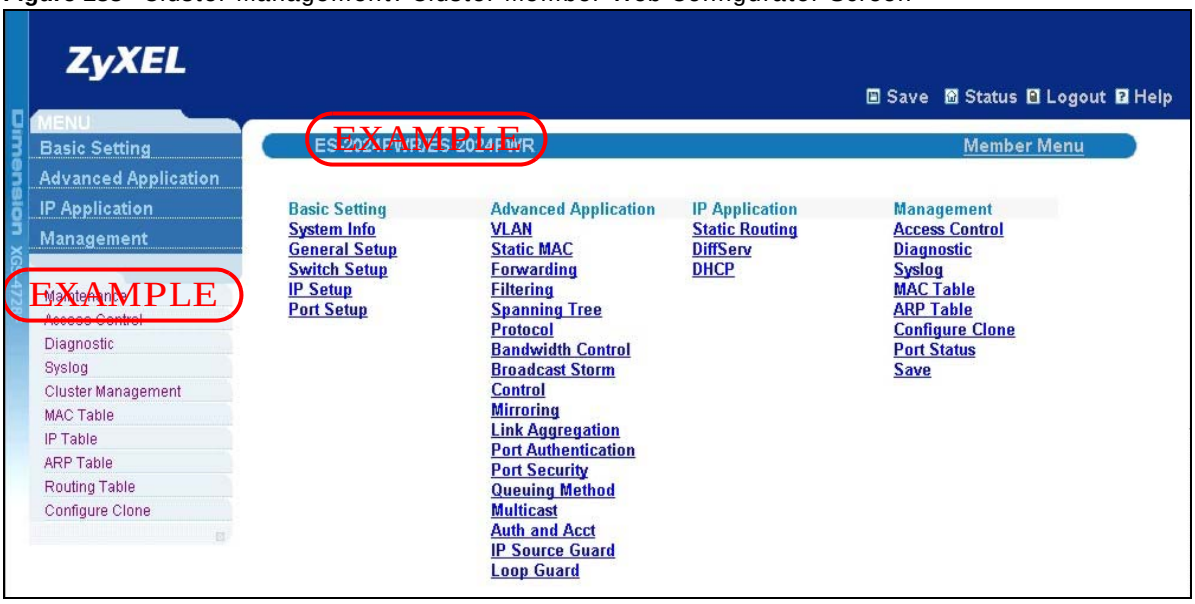
LABEL	DESCRIPTION
Status	This field displays the role of this Switch within the cluster. **Manager** **Member** (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) **None** (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the **Index** column is a hyperlink leading to the cluster member switch's web configurator (see Figure 188 on page 303).
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This field displays the model name.
Status	This field displays: **Online** (the cluster member switch is accessible) **Error** (for example, the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) **Offline** (the switch is disconnected - **Offline** shows approximately 1.5 minutes after the link between cluster member and manager goes down)

39.2.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's web

configurator home page. This cluster member web configurator home page and the home page that you'd see if you accessed it directly are different.

Figure 188 Cluster Management: Cluster Member Web Configurator Screen



39.2.1.1 Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

Figure 189 Example: Uploading Firmware to a Cluster Member Switch

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 Switch FTP version 1.0 ready at Thu Jan  1 00:58:46 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-   1 owner    group         3042210 Jul 01 12:00 ras
-rw-rw-rw-   1 owner    group          393216 Jul 01 12:00 config
--w--w--w-   1 owner    group               0 Jul 01 12:00 fw-00-a0-c5-01-23-46
-rw-rw-rw-   1 owner    group               0 Jul 01 12:00 config-00-a0-c5-01-23-46
226 File sent OK
ftp: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 400AAEW0C0.bin fw-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR fw-00-a0-c5-01-23-46
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

The following table explains some of the FTP parameters.

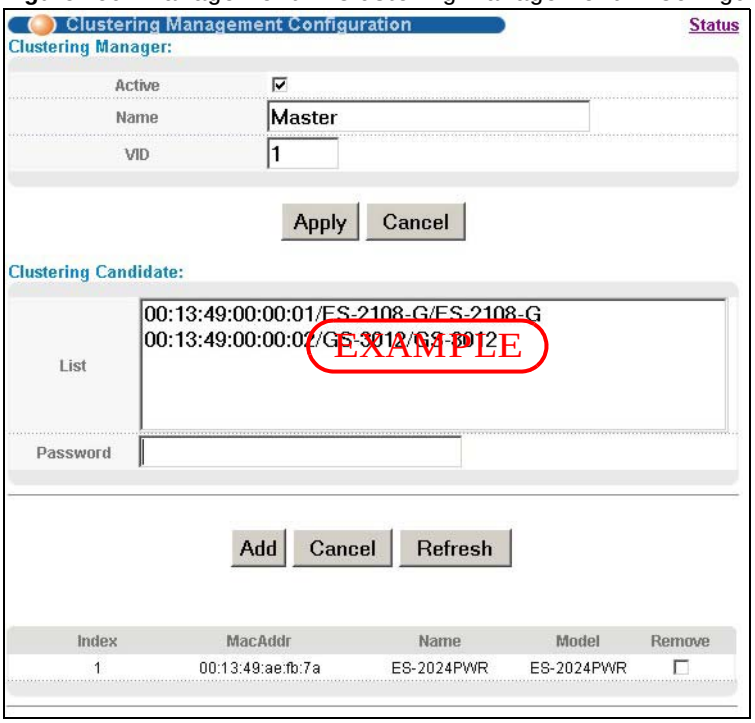
Table 147 FTP Upload to Cluster Member Example

FTP PARAMETER	DESCRIPTION
User	Enter “admin”.
Password	The web configurator password default is 1234.
ls	Enter this command to list the name of cluster member switch’s firmware and configuration file.
400AAEW0C0.bin	This is the name of the firmware file you want to upload to the cluster member switch.
fw-00-a0-c5-01-23-46	This is the cluster member switch’s firmware name as seen in the cluster manager switch.
config-00-a0-c5-01-23-46	This is the cluster member switch’s configuration file name as seen in the cluster manager switch.

39.3 Clustering Management Configuration

Use this screen to configure clustering management. Click **Configuration** from the **Cluster Management** screen to display the next screen.

Figure 190 Management > Clustering Management > Configuration



The following table describes the labels in this screen.

Table 148 Management > Clustering Management > Configuration

LABEL	DESCRIPTION
Clustering Manager	
Active	Select **Active** to have this Switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the **Clustering Candidates** list. If a switch that was previously a cluster member is later set to become a cluster manager, then its **Status** is displayed as **Error** in the **Cluster Management Status** screen appears in the member summary list below.
Name	Type a name to identify the **Clustering Manager**. You may use up to 32 printable characters (spaces are allowed).
VID	This is the VLAN ID and is only applicable if the Switch is set to **802.1Q** VLAN. All switches must be directly connected and in the same VLAN group to belong to the same cluster. Switches that are not in the same VLAN group are not visible in the **Clustering Candidates** list. This field is ignored if the **Clustering Manager** is using **Port-based** VLAN.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the **Clustering Candidate** list. Switches that are not in the same management VLAN group will not be visible in the **Clustering Candidate** list.
Password	Each cluster member's password is its web configurator password. Select a member in the **Clustering Candidate** list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the **Cluster Manager**. Its **Status** is displayed as **Error** in the **Cluster Management Status** screen. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Add	Click **Add** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Refresh	Click **Refresh** to perform auto-discovery again to list potential cluster members.
The next summary table shows the information for the clustering members configured.	
Index	This is the index number of a cluster member switch.
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's **System Name**.
Model	This is the cluster member switch's model name.
Remove	Select this checkbox and then click the **Remove** button to remove a cluster member switch from the cluster.
Cancel	Click **Cancel** to begin configuring this screen afresh.

40

MAC Table

This chapter introduces the **MAC Table** screen.

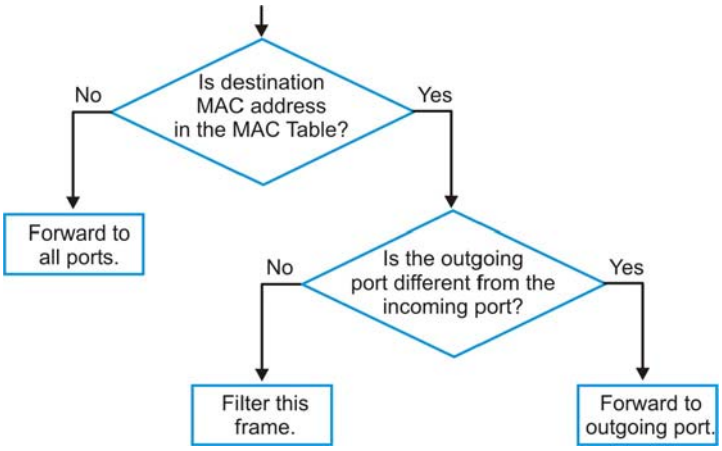
40.1 MAC Table Overview

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the MAC address of the device is shown on the Switch's **MAC Table**. It also shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

The Switch uses the **MAC Table** to determine how to forward frames. See the following figure.

1. The Switch examines a received frame and learns the port from which this source MAC address came.
2. The Switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the **MAC Table**.
   - If the Switch has already learned the port for this MAC address, then it forwards the frame to that port.
   - If the Switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
   - If the Switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

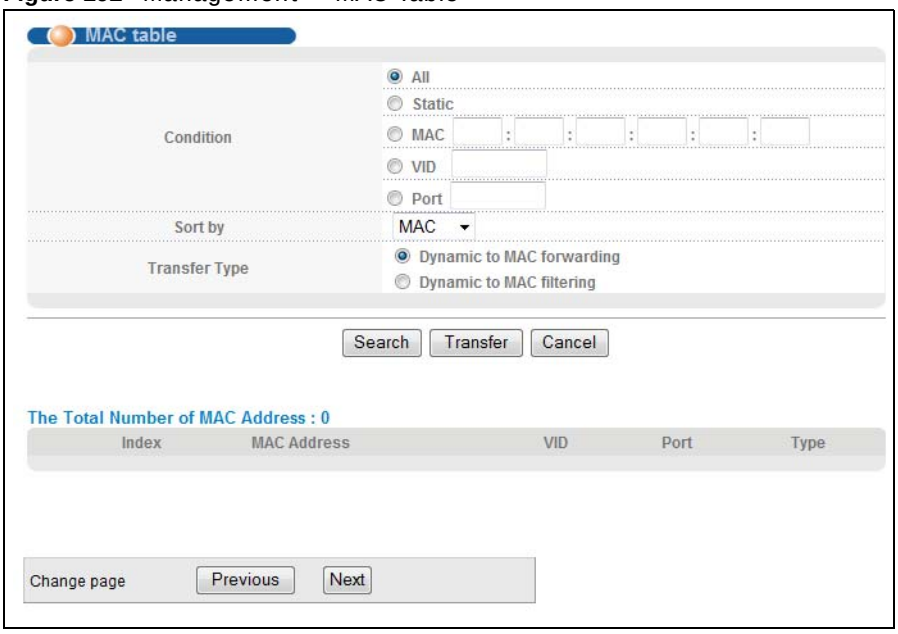
Figure 191 MAC Table Flowchart



40.2 Viewing the MAC Table

Click **Management** > **MAC Table** in the navigation panel to display the following screen. Use this screen to search specific MAC addresses. You can also directly add dynamic MAC address(es) into the static MAC forwarding table or MAC filtering table from the MAC table using this screen.

Figure 192 Management > MAC Table



The following table describes the labels in this screen.

Table 149 Management > MAC Table

LABEL	DESCRIPTION
Condition	Select **All** to display all MAC addresses in the MAC table. Select **Static** to only display static MAC address(es) in this screen. Select **MAC** and enter a valid MAC address (six hexadecimal character pairs) to display the MAC address information in this screen. Select **VID** and type a VLAN identification number to display all MAC addresses in the VLAN. Select **Port** and type the number of a port to display all MAC addresses learned from the port.
Sort by	Select this to display and arrange the data according to MAC address (**MAC**), VLAN group (**VID**) or port number (**Port**). The information is then displayed in the summary table below.
Transfer Type	Select **Dynamic to MAC forwarding** and click **Transfer** to add the relative dynamic MAC address(es) you select the criteria here into the static MAC forwarding table (see Section 8.2 on page 99). The type of the MAC address(es) will be changed to “static”. Select **Dynamic to MAC filtering** and click **Transfer** to add the relative dynamic MAC address(es) you make the search here into the static MAC filtering table (see Section 10.1 on page 105). The MAC address(es) will be removed from the MAC table and all traffic sent from the MAC address(es) will be blocked by the Switch.
Search	Click this to search data in the MAC table according to your input criteria.

Table 149 Management > MAC Table (continued)

LABEL	DESCRIPTION
Transfer	Click this to perform the MAC address transferring you selected in the **Transfer Type** field.
Cancel	Click this to begin configuring the search criteria afresh.
The Total Number of MAC Address	This field displays the total number of MAC addresses learned on the Switch.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port from which the above MAC address was learned.
Type	This shows whether the MAC address is **dynamic** (learned by the Switch) or **static** (manually entered in the **Static MAC Forwarding** screen).
Change Pages	Click **Previous** or **Next** to show the previous/next screen if all status information cannot be seen in one screen.

41

ARP Table

This chapter introduces ARP Table.

41.1 ARP Table Overview

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

41.1.1 How ARP Works

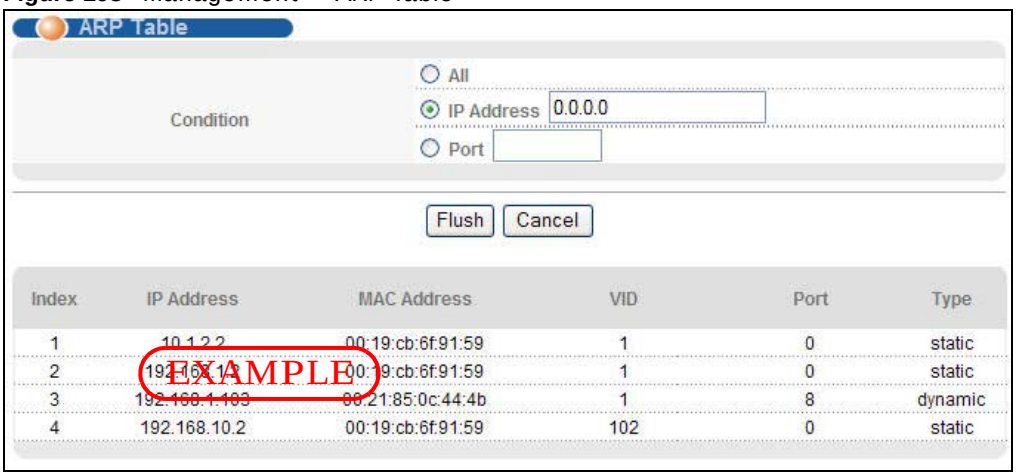
When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch's ARP program looks in the ARP Table and if it finds the address, it sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

41.2 The ARP Table Screen

Click **Management** > **ARP Table** in the navigation panel to open the following screen. Use the ARP table to view IP-to-MAC address mapping(s) and remove specific dynamic ARP entries.

Figure 193 Management > ARP Table



The following table describes the labels in this screen.

Table 150 Management > ARP Table

LABEL	DESCRIPTION
Condition	Specify how you want the Switch to remove ARP entries when you click **Flush**. Select **All** to remove all of the dynamic entries from the ARP table. Select **IP Address** and enter an IP address to remove the dynamic entries learned with the specified IP address. Select **Port** and enter a port number to remove the dynamic entries learned on the specified port.
Flush	Click **Flush** to remove the ARP entries according to the condition you specified.
Cancel	Click **Cancel** to return the fields to the factory defaults.
Index	This is the ARP table entry number.
IP Address	This is the learned IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
VID	This field displays the VLAN to which the device belongs.
Port	This field displays the port to which the device connects. **CPU** means this learned IP address is the Switch's management IP address.
Type	This shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

42

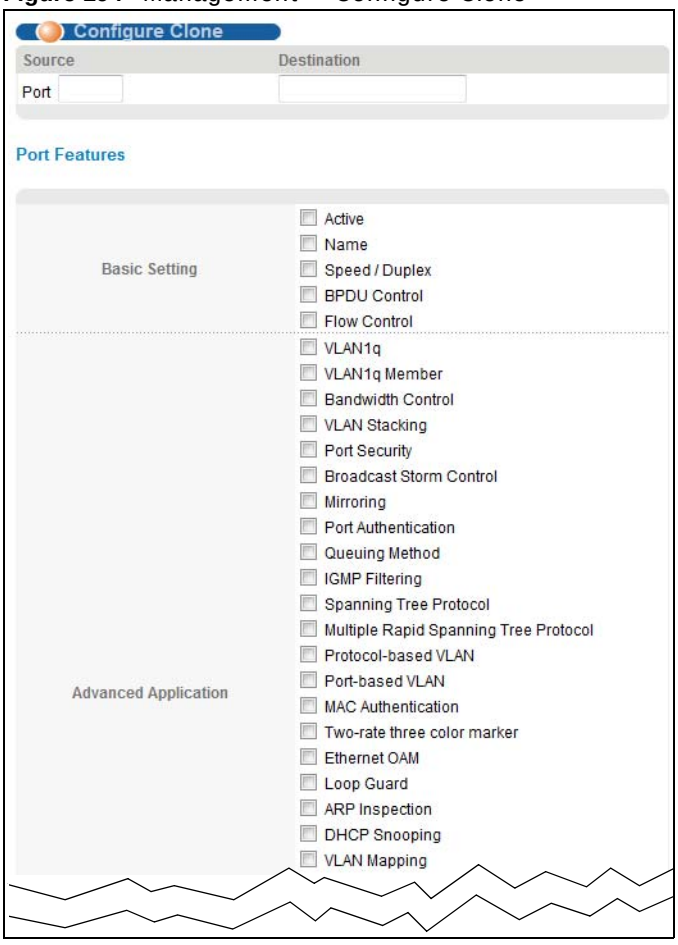
Configure Clone

This chapter shows you how you can copy the settings of one port onto other ports.

42.1 Configure Clone

Cloning allows you to copy the basic and advanced settings from a source port to a destination port or ports. Click **Management** > **Configure Clone** to open the following screen.

Figure 194 Management > Configure Clone



The following table describes the labels in this screen.

Table 151 Management > Configure Clone

LABEL	DESCRIPTION
Source/ Destination Port	Enter the source port under the **Source** label. This port's attributes are copied. Enter the destination port or ports under the **Destination** label. These are the ports which are going to have the same attributes as the source port. You can enter individual ports separated by a comma or a range of ports by using a dash. Example: • **2, 4, 6** indicates that ports 2, 4 and 6 are the destination ports. • **2-6** indicates that ports 2 through 6 are the destination ports.
Basic Setting	Select which port settings (configured in the **Basic Setting** menus) should be copied to the destination port(s).
Advanced Application	Select which port settings (configured in the **Advanced Application** menus) should be copied to the destination ports.
Apply	Click **Apply** to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the **Save** link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

43

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Switch Access and Login
- Switch Configuration

43.1 Power, Hardware Connections, and LEDs

The Switch does not turn on. None of the LEDs turn on.

1. Make sure the Switch is turned on.
2. Make sure you are using the power adaptor or cord included with the Switch.
3. Make sure the power adaptor or cord is connected to the Switch and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the Switch off and on.
5. Disconnect and re-connect the power adaptor or cord to the Switch (in AC models or if the AC power supply is connected in AC/DC models).
6. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 3.3 on page 52.
2. Check the hardware connections. See Section 3.1 on page 49.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the Switch off and on (in DC models or if the DC power supply is connected in AC/DC models).

5 Disconnect and re-connect the power adaptor or cord to the Switch (in AC models or if the AC power supply is connected in AC/DC models).

6 If the problem continues, contact the vendor.

43.2 Switch Access and Login

I forgot the IP address for the Switch.

1 The default in-band IP address is **192.168.1.1**.

2 Use the console port to log in to the Switch.

3 Use the **MGMT** port to log in to the Switch, the default IP address of the **MGMT** port is 192.168.0.1.

4 If this does not work, you have to reset the device to its factory defaults. See Section 4.6 on page 59.

I forgot the username and/or password.

1 The default username is **admin** and the default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 4.6 on page 59.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default in-band IP address is 192.168.1.1.
- If you changed the IP address, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Switch.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 3.3 on page 52.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.

4 Make sure your computer is in the same subnet as the Switch. (If you know that there are routers between your computer and the Switch, skip this step.)

5 Reset the device to its factory defaults, and try to access the Switch with the default IP address. See Section 4.6 on page 59.

6 If the problem continues, contact the vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the Switch using another service, such as Telnet. If you can access the Switch, check the remote management settings to find out why the Switch does not respond to HTTP.

I can see the **Login** screen, but I cannot log in to the Switch.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later.

Check that you have enabled logins for HTTP or Telnet. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.

3 Disconnect and re-connect the cord to the Switch.

4 If this does not work, you have to reset the device to its factory defaults. See Section 4.6 on page 59.

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

I cannot see some submenus at the bottom of the navigation panel.

The recommended screen resolution is 1024 by 768 pixels. Adjust the value in your computer and then you should see the rest of the submenus at the bottom of the navigation panel.

There is unauthorized access to my Switch via telnet, HTTP and SSH.

Click the **Display** button in the **System Log** field in the **Management** > **Diagnostic** screen to check for unauthorized access to your Switch. To avoid unauthorized access, configure the secured client setting in the **Management** > **Access Control** > **Remote Management** screen for telnet, HTTP and SSH (see Section 36.6 on page 294). Computers not belonging to the secured client set cannot get permission to access the Switch.

43.3 Switch Configuration

I lost my configuration settings after I restart the Switch.

Make sure you save your configuration into the Switch's nonvolatile memory each time you make changes. Click **Save** at the top right corner of the web configurator to save the configuration permanently. See also Section 35.3 on page 270 for more information about how to save your configuration.

A

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **User-Defined**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 152 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.

Table 152 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).

Table 152 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

B

Legal Information

Copyright

Copyright © 2013 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications (Class A)

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.

- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- For continued protection against risk of fire replace only with same type and rating of fuse.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Index

Numbers

802.1P priority 79

A

access control
  limitations 276
  login account 285
  remote management 294
  service port 293
  SNMP 276
accounting
  setup 193
address learning, MAC 90, 92
Address Resolution Protocol (ARP) 309, 311, 312
administrator password 286
age 120
aggregator ID 135, 137
aging time 74
applications
  bridging 21
  IEEE 802.1Q VLAN 22
  switched workgroup 22
ARP
  how it works 309
  table 310
ARP (Address Resolution Protocol) 309
ARP inspection 200, 203
  and MAC filter 203
  configuring 204
  syslog messages 204
  trusted ports 203, 204
authentication
  and RADIUS 188
  setup 193
authorization
  privilege levels 195
  setup 193
automatic VLAN registration 82

B

back up, configuration file 272
basic settings 70
basic setup tutorial 25
binding 200
binding table 200
  building 200
BPDUs (Bridge Protocol Data Units) 108
Bridge Protocol Data Units (BPDUs) 108

C

CDP 230
certifications
  notices 321
  viewing 321
CFI (Canonical Format Indicator) 81
changing the password 58
Cisco Discovery Protocol, see CDP
CIST 111
CIST (Common and Internal Spanning Tree) 109
Class of Service (CoS) 256
classifier 151, 153
  and QoS 151
  editing 154
  example 156
  overview 151
  setup 151, 153, 154
  viewing 154
CLI
  Reference Guide 2
cloning a port See port cloning
cluster management 300
  and switch passwords 305
  cluster manager 300, 305
  cluster member 300, 305
  cluster member firmware upgrade 303
  network example 301

setup 304
specification 300
status 301
switch models 300
VID 305
web configurator 302
cluster manager 300
cluster member 300
command interface 23
Common and Internal Spanning Tree (CIST) 109
Common and Internal Spanning Tree, See CIST 111
configuration 255
change running config 270
configuration file 59
backup 272
restore 59, 272
saving 270
configuration, saving 59
copying port settings, See port cloning
copyright 321
CPU management port 95
CPU protection
configuration 245
overview 244
current date 73
current time 73

D

dac10g 79
Data Center Bridging (DCB) 17, 19
DCBX 20
ETS 19
PFC 18, 20
daylight saving time 73
DCBX 18
DHCP 263
configuration options 263
relay example 267
setup 266
DHCP (Dynamic Host Configuration Protocol) 263
DHCP relay option 82 202
DHCP snooping 25, 200, 201
configuring 202
DHCP relay option 82 202
trusted ports 201
untrusted ports 201
DHCP snooping database 201
diagnostics 296
Ethernet port test 296
ping 296
system log 296
Differentiated Service (DiffServ) 256
DiffServ 256
activate 258
and TRTCM 260
DS field 256
DSCP 256
DSCP-to-IEEE802.1p mapping 261
network example 256
PHB 256
Direct Attach Copper (DAC) 49, 79
disclaimer 321
documentation
related 2
double-tagged frames 165
DS (Differentiated Services) 256
DSCP
DSCP-to-IEEE802.1p mapping 261
service level 256
what it does 256
DSCP (DiffServ Code Point) 256
dynamic link aggregation 132

E

egress port 98
Error Disable 38
error disable detect 246
error disable recovery
configuration 247
overview 244
Ethernet broadcast address 309
Ethernet port test 296
ETS 18
external authentication server 188

F

fan speed 71
file transfer using FTP
  command example 273
filename convention, configuration
  configuration
    file names 273
filtering 105
  rules 105
filtering database, MAC table 306
firmware 71
  upgrade 271, 303
flow control 79
  back pressure 79
  IEEE802.3x 79
forwarding
  delay 120
frames
  tagged 89
  untagged 89
front panel 49
FTP 23, 273
  file transfer procedure 274
  restrictions over WAN 274

G

GARP 82
GARP (Generic Attribute Registration Protocol) 82
GARP terminology 82
GARP timer 75, 82
general setup 72
getting help 61
GMT (Greenwich Mean Time) 73
Guide
  CLI Reference 2
GVRP 82, 88, 89
  and port assignment 89
GVRP (GARP VLAN Registration Protocol) 82

H

hardware monitor 71
hello time 120
hops 120
HTTPS 288
  certificates 288
  implementation 288
  public keys, private keys 288
HTTPS example 289

I

IEEE 802.1p, priority 75
IEEE 802.1x
  activate 143, 146, 191
  reauthentication 144
IEEE 802.1x, port authentication 140
IGMP
  version 172
IGMP (Internet Group Management Protocol) 172
IGMP filtering 172
  profile 178
  profiles 174
IGMP leave timeout
  fast 175
  mormal 175
IGMP snooping 172
  MVR 179
IGMP throttling 176
ingress port 98
Internet Protocol version 6, see IPv6
introduction 17
IP
  setup 76
IP source guard 200
  ARP inspection 200, 203
  DHCP snooping 200, 201
  static bindings 200
IPv6 23
  Neighbor Discovery Protocol 23
  ping 23

L

L2PT 228
  access port 229
  CDP 228
  configuration 230
  encapsulation 228
  LACP 229
  MAC address 228
  mode 229
  overview 228
  PAgP 229
  point to point 229
  STP 228
  tunnel port 229
  UDLD 229
  VTP 228
LACP 132, 231
  system priority 138
  timeout 138
Layer 2 protocol tunneling, see L2PT
LEDs 52
limit MAC address learning 149
Link Aggregate Control Protocol (LACP) 132
link aggregation 132
  dynamic 132
  ID information 133
  setup 135, 137
  status 133
  traffic distribution algorithm 134
  traffic distribution type 136
lockout 59
log 296
login 53
  password 58
login account
  Administrator 285
  non-administrator 286
login accounts 285
  configuring via web configurator 285
  multiple 285
  number of 285
login password 286
loop guard 220
  how it works 221
  port shut down 222
  probe packet 221
loop guard, vs STP 220

M

MAC (Media Access Control) 71
MAC address 71, 309
  maximum number per port 149, 150
MAC address learning 74, 90, 92, 99, 149
  specify limit 149
MAC authentication 141
  aging time 147
MAC filter
  and ARP inspection 203
MAC freeze 149
MAC table 306
  how it works 306
  viewing 307
maintanence
  configuration backup 272
  firmware 271
  restoring configuration 272
maintenance 269
  current configuration 269
  main screen 269
Management Information Base (MIB) 277
management port 98
managing the device
  good habits 24
  using FTP. See FTP.
  using SNMP. See SNMP.
  using Telnet. See command interface.
  using the command interface. See command interface.
  using the web configurator. See web configurator.
man-in-the-middle attacks 203
max
  age 120
  hops 120
MIB
  and SNMP 277
  supported MIBs 278
MIB (Management Information Base) 277
mirroring ports 130
monitor port 130
MSA (MultiSource Agreement) 50

MST Instance, See MSTI 111
MST region 110
MSTI 111
  MST ID 111
MSTI (Multiple Spanning Tree Instance) 109
MSTP 107, 109
  bridge ID 123, 124
  configuration 119, 122
  configuration digest 124
  forwarding delay 120
  Hello Time 123
  hello time 120
  Max Age 123
  max age 120
  max hops 120
  MST region 110
  network example 110
  path cost 121
  port priority 121
  revision level 120
MSTP (Multiple Spanning Tree Protocol) 107
MTU (Multi-Tenant Unit) 73
multicast 172
  802.1 priority 174
  and IGMP 172
  IGMP throttling 176
  IP addresses 172
  overview 172
  setup 174
multicast group 178
multicast VLAN 183
Multiple Spanning Tree Instance, See MSTI 109
Multiple Spanning Tree Protocol 108
Multiple Spanning Tree Protocol, See MSTP. 107
Multiple STP 108
Multiple STP, see MSTP 109
MVR 179
  configuration 181
  group configuration 183
  network example 179
MVR (Multicast VLAN Registration) 179

N

network management system (NMS) 276
NTP (RFC-1305) 72

O

other documentation 2

P

PAGP 231
password 58
  administrator 286
PHB (Per-Hop Behavior) 256
ping, test connection 296
policy 158, 160
  and classifier 158
  and DiffServ 157
  configuration 158
  example 161
  overview 157
  rules 157
  viewing 160
policy configuration 160
Port Aggregation Protocol, see PAgP
port authentication 140
  and RADIUS 188
  IEEE802.1x 143, 146, 191
  MAC authentication 141
port based VLAN type 74
port cloning 311, 312
  advanced settings 311, 312
  basic settings 311, 312
port details 66
port isolation 98
port mirroring 130
  direction 131
  egress 131
  ingress 131
port redundancy 132
port security 148
  address learning 149
  limit MAC address learning 149
  MAC address learning 148
  overview 148
  setup 148, 222, 230

port setup 78
port status 65
port VLAN trunking 83
port-based VLAN 95
  all connected 98
  port isolation 98
  settings wizard 98
ports
  “standby” 132
  diagnostics 296
  mirroring 130
  speed/duplex 79
power
  voltage 71
power status 71
PPPoE IA 33
  trusted ports 238
  untrusted ports 238
priority level 75
priority, queue assignment 75
Private VLAN Status 94
product registration 321
protocol based VLAN 91
  and IEEE 802.1Q tagging 91
  example 93
  hexadecimal notation for protocols 91, 92
  isolate traffic 91
  priority 91, 92
PVID 81, 89
PVID (Priority Frame) 81

Q

QoS
  and classifier 151
QSFP+ 49
queue weight 163
queuing 162
  SPQ 163
  WFQ 163
  WRR 163
queuing method 162, 164

R

RADIUS 188
  advantages 188
  and authentication 188
  Network example 187
  server 188
  settings 188
  setup 188
Rapid Spanning Tree Protocol, See RSTP. 107
reboot
  load configuration 270
reboot system 270
Reference Guide, CLI 2
registration
  product 321
related documentation 2
remote management 294
  service 295
  trusted computers 295
resetting 59, 270
  to factory default settings 270
restoring configuration 59, 272
RFC 3164 297
Round Robin Scheduling 163
RSTP 107

S

save configuration 59, 270
Secure Shell See SSH
service access control 293
  service port 294
sFlow 232
  collector 234
  configuration 233
  datagram 232
  overview 232
  poll interval 233
  sample rate 233
  UDP port 234
sFlow agent 232
sFlow collector 232
sfp_plus 79
SFP+ 49

SFP+ Direct Attach Copper (DAC) 79
SFP+ ports
transceiver removal 50
Simple Network Management Protocol, see SNMP
SNMP 24, 276
agent 277
and MIB 277
authentication 285
communities 282
management model 277
manager 277
MIB 278
network components 277
object variables 277
protocol operations 277
security 284, 285
setup 282
traps 283
users 284
version 3 and security 277
versions supported 276
SNMP traps 278
supported 278, 280, 281
Spanning Tree Protocol, See STP. 107
SPQ (Strict Priority Queuing) 163
SSH
encryption methods 288
how it works 287
implementation 288
SSH (Secure Shell) 287
SSL (Secure Socket Layer) 288
standby ports 132
static bindings 200
static MAC address 99
static MAC forwarding 90, 92, 99
static multicast address 101
static multicast forwarding 101
static route
configuration 254
static routes 255
static trunking example 138
Static VLAN 86
static VLAN
control 87
tagging 87
status 65
LED 52
link aggregation 133
port 65
port details 66
power 71
STP 114, 117, 123
VLAN 84
STP 107, 231
bridge ID 115, 118
bridge priority 113, 116
configuration 113, 116, 119
designated bridge 108
forwarding delay 114, 117
Hello BPDU 108
Hello Time 113, 115, 117, 118
how it works 108
Max Age 114, 115, 117, 118
path cost 107, 114, 117
port priority 114, 117
port state 108
root port 108
status 114, 117, 123
terminology 107
vs loop guard 220
subnet based VLANs 89
and DHCP VLAN 91
and priority 89
configuration 90
switch hardware overview 49
switch lockout 59
switch reset 59
switch setup 74
syslog 204, 297
protocol 297
server setup 299
settings 298
setup 298
severity levels 297
system information 70
system log 296
system reboot 270

T

TACACS+ 188
setup 191

TACACS+ (Terminal Access Controller Access-Control System Plus) 187
tagged VLAN 81
temperature indicator 71
time
  current 73
  time zone 73
Time (RFC-868) 72
time server 72
time service protocol 72
  format 72
trademarks 321
transceiver
  installation 50
  removal 50
transceiver ports
  connection speed 50
  connector type 50
  transceiver installation 50
Transceivers 49
traps
  destination 282
TRTCM
  and bandwidth control 260
  and DiffServ 260
  color-aware mode 258
  color-blind mode 258
  setup 259
trunk group 132
trunking 132
  example 138
trusted ports
  ARP inspection 203
  DHCP snooping 201
  PPPoE IA 238
Tunnel Protocol Attribute, and RADIUS 196
tutorials 25
  DHCP snooping 25
  Error Disable 38
  PPPoE IA 33
Two Rate Three Color Marker (TRTCM) 257
Two Rate Three Color Marker, see TRTCM 257
Type of Service (ToS) 256

U

UDLD 231
UniDirectional Link Detection, see UDLD
untrusted ports
  ARP inspection 204
  DHCP snooping 201
  PPPoE IA 238
user profiles 187

V

Vendor Specific Attribute See VSA
VID 81, 84, 85, 167
  number of possible VIDs 81
  priority frame 81
VID (VLAN Identifier) 81
VLAN 73, 81
  acceptable frame type 89
  automatic registration 82
  ID 81
  ingress filtering 88
  introduction 73
  number of VLANs 84
  port number 85
  port settings 88
  port-based VLAN 95
  port-based, all connected 98
  port-based, isolation 98
  port-based, wizard 98
  static VLAN 86, 94
  status 84, 85
  tagged 81
  trunking 83, 89
  type 74, 83
VLAN (Virtual Local Area Network) 73
VLAN mapping 224
  activating 225
  configuration 226
  example 224
  priority level 224
  tagged 224
  traffic flow 224
  untagged 224
  VLAN ID 224
VLAN number 77

VLAN stacking 165, 167
configuration 168
example 165
frame format 167
port roles 166, 168
port-based Q-in-Q 169
priority 167
selective Q-in-Q 170
VLAN Trunking Protocol, see VTP
VLAN, protocol based, See protocol based VLAN
VLAN, subnet based, See subnet based VLANs 89
VSA 195
VTP 231

W

warranty 321
note 321
web configurator 23, 53
getting help 61
layout 54
login 53
logout 61
navigation panel 56
weight, queuing 163
Weighted Round Robin Scheduling (WRR) 163
WFQ (Weighted Fair Queuing) 163
WRR (Weighted Round Robin Scheduling 163

Z

ZyNOS (ZyXEL Network Operating System) 273